SYMANTEC®

ServiceDesk Customization Guide 7.0

Symantec ServiceDesk 7

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 2, revised 24 March 2010

Legal Notice

Copyright © 2010 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, and Altiris are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

www.symantec.com/techsupp/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
    - Error messages and log files
    - Troubleshooting that was performed before contacting Symantec
    - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and maintenance contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

Asia-Pacific and Japan	contractsadmin@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.

Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Technical Support 3

Introduction 8
Intended Audience 8
ServiceDesk 7 High-Level Capabilities 8
Relationship Between ServiceDesk 7 & Symantec Workflow 9
Process Manager (ServiceDesk) Database 9
Relationship Between ServiceDesk 7 & Altiris Notification Server (NS) Computer 9
Best Practice: Keep It Simple in the Beginning 10
Phases in Implementing ServiceDesk 10

Phase 1: Process and Workflow Planning 11
Step 1: Select Pieces of ServiceDesk 7 to Use 11
Step 2: Identify Current Processes 12

Phase 2: Installation, Configuration, and Basic Customization 13
Installation & Configuration 13
Notification Server 13
ServiceDesk 7 13
Versioning Processes 14
Pros and Cons of Writing to the Same Virtual Directory 15
Development Considerations When Publishing to the Same Virtual Directory 16
Basic Steps for Versioning 16
About Application Properties 17
Restoring ServiceDesk Processes 17
Project Differential Tool 18
Basic ServiceDesk 7 Customization 18
Editing the Core ITIL Processes 18
Verify Users, Groups, and Organizations 18
Set Up Incident Categories (Classifications) 19
Verify Default Priority, Impact, and Urgency Values 20
Verify Close Codes 23
Portal Master Settings 23
Customize the General Appearance of the Portal 24
Customize Form Appearance & Content 25
Establish Routing (Assignment) of Incidents 29
Establish Service Level Agreement (SLA) Times 33
Set Business Hours & Holidays 35
Set Up "Follow the Sun" 37
Change the Frequency of the Customer Service Satisfaction Survey 37
Define Quick Incident Templates 38
Define E-mail Content 39
Customize E-mail Monitoring 40
Modify the Timespan for End-Users to Confirm Incident Resolution 42
Add a Cube Report Schedule 42
Establish Change Management Groups 43
Change Risk Assessment Participation for Change Management 43
Verify Problem Categories 45

Phase 3: Advanced Customization 46
Extend Data/Profiles 46
About SD.Data 46
Extend the ServiceDesk Incident Data Type 46
Extend the CustomerServiceSurvey Data Type 48
Extend the Change Request Data Type 48
Extend the ServiceDesk Problem Data Type 48
Add & Customize Pages 49
Modify Types of Changes 49
Define Smart Tasks 50
Add Smart Tasks to the Initial Diagnosis Dialog Workflow 51
Add to the Service Catalog 53
Define New Reports 53
Creating a Child Report 55
Configure Automatic Generation of Reports 55
Making a Report a Web Service 55
Replicating ServiceDesk Data 56
Create a New Schedule 56
Adding & Removing E-mail Notification 57
Application Property for Two Notifications 58
Remove an Approval Step 58
Customize the Spell Checking Dictionary 58
Create Incidents from Other Sources 59
Notification Server 59
Other Systems 59
Integrate ServiceDesk 7 with Other Systems 59
Create a Web Part 60
Non-Changeable Items in Symantec Workflow Projects 63
Scalability 64
ServiceDesk 7 Configurations 65

Introduction

With Symantec® ServiceDesk 7 software, you can provide the level of service that your organization expects and can afford, keeping hundreds—even tens of thousands—of computers running efficiently, while providing new services on a regular basis.

The key is to create an organized environment that quickly responds to reported issues, and, at the same time, advertises and provides new services to the organization. The ultimate goal is to provide better service by automating as many steps as possible, and, where automation isn't possible, to increase the efficiency of the people who provide the services.

Intended Audience

This guide (particularly sections 2 and 3), is for administrative users who plan to customize ServiceDesk 7 on their own. You can also leverage experienced consultants to help.

Note:
It is required that you have working knowledge of Symantec Workflow in order to perform many of the configuration steps explained in this document.

ServiceDesk 7 High-Level Capabilities

ServiceDesk 7 can be configured to capture issues electronically through e-mail or from other applications, or through special Web-based screens designed for end-users or technicians to log an incident. End-users receive updates on all problems that they report. Once an issue is reported, it can be prioritized and routed to the right people who can solve the problem and report the success back to the users and management.

ServiceDesk 7 has many automated capabilities that can drive down the amount of human effort needed to correct issues. In other cases, where several people need to be involved in the process, such as purchasing, installing, and provisioning a new server, ServiceDesk 7 can provide coordination between all of the parties to help eliminate delays and improve service levels. ServiceDesk 7 can then become a central communication and coordination center for all of the things going on in the IT department, and in many cases it can extend beyond IT to provide services to Facilities, Telecommunications, Human Resources, Equipment Maintenance, and so on.

An IT process is a predefined series of steps that are executed in a repeatable way to deliver the same expected outcome each time the process is triggered. When a company can move from a place where IT problems are solved in an ad-hoc manner to one where every issue is handled in an efficient and repeatable manner, cost goes down and end user satisfaction goes up.

A workflow is the implementation of an IT process in ServiceDesk 7. Workflows are housed in projects, built in the Symantec Workflow software.

Relationship Between ServiceDesk 7 & Symantec Workflow

ServiceDesk 7 relies upon Symantec Workflow software to drive the core ServiceDesk 7 ITIL processes, and the Service Catalog and Knowledge Base process. Symantec Workflow is a critical technology to understand, as it is fundamental to the functionality and customization of ServiceDesk 7. Most customization explained in this document is done using this tool.

ServiceDesk 7 processes are contained in Symantec Workflow projects that are provided by the ServiceDesk 7 installation.

ServiceDesk 7 follows a different paradigm than other helpdesk applications in that it is driven by process, not by data. The process enforces the rules. Symantec took great care in creating the processes, taking into account customer feedback and ITIL best practice recommendations.

Note that changes to a Symantec Workflow project require testing and deployment to production in order for the changes to become visible to ServiceDesk 7 users. The instructions in this document cover the basics of deployment, but more in-depth instructions on it and using the Debugger for testing are covered in the Symantec Workflow documentation.

Process Manager (ServiceDesk) Database

The term "Process Manager" refers to the database that stores process data, and ServiceDesk data such as groups, users, and permissions. The Process Manager database is a standard part of Symantec Workflow; when you install ServiceDesk, it is expanded to become the ServiceDesk database (however it is commonly referred to as "Process Manager"). This database resides on the SQL Server computer.

Relationship Between ServiceDesk 7 & Altiris Notification Server (NS) Computer

Note:
Symantec Management Platform 7.0 is the product installed on the NS computer that manages the licensing.

Previous versions of Altiris HelpDesk used the Notification Server computer to define business rules; now all of these are handled in Symantec Workflow. ServiceDesk 7 relies upon Altiris Notification Server for three functions:

- Licensing information,
- IT asset locations, conifigurations, and historical information, and,
- Exposure to the Configuration Management Database (CMDB).

It is required to have Notification Server computer up and running, and configured, prior to implementing ServiceDesk 7.

Best Practice: Keep It Simple in the Beginning

Out-of-the-box, ServiceDesk is intended to require little customization; use this guide as a checklist to identify the most important aspects to customize.

Keep the initial implementation of ServiceDesk 7 simple enough for most of your staff to understand and manage. Aim to provide the basic functionality and services needed to achieve a reasonable amount of satisfaction, not the ultimate "end all" solution. Then, build up the ServiceDesk 7 system over time as the support staff and the end-users become more familiar with it.

Phases in Implementing ServiceDesk

This document organizes the process of implementing ServiceDesk 7 into 3 phases.

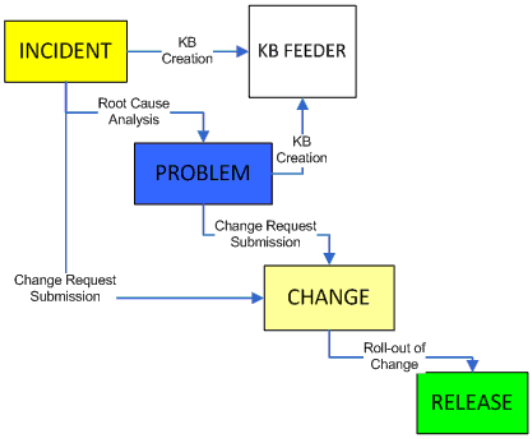
- *Phase 1: Process and Workflow Planning* (page 11)
- *Phase 2: Installation, Configuration, and Basic Customization* (page 13)
- *Phase 3: Advanced Customization* (page 46)

Phase 1: Process and Workflow Planning

In this initial phase, you consider the processes that you want to use in ServiceDesk 7. There are the four core ITIL processes (Incident Management, Change Management, Problem Management, and Release Management), a Service Catalog, and Knowledge Base process; you may or may not want to use all of these.

You also want to map out your current process so you can identify where customizations need to be made in the "out of the box" ServiceDesk 7 processes.

Step 1: Select Pieces of ServiceDesk 7 to Use



The following explanations will help you determine what processes you want to use in ServiceDesk 7. Most clients will use Incident Management at a minimum. These processes directly follow Symantec's opinion of ITIL best practices, determined through customer feedback and scrutiny of ITIL documentation.

- Incident Management Process

  The incident management process manages incidents with a focus on restoring the user to an operational state as quickly as possible to the level identified in the Service Level Agreement.

- Problem Management Process

  The problem management process aims to reduce the occurrence and negative impact of incidents that are reported to the ServiceDesk. The process looks proactively for trends in the environment to identify the root cause of incidents and initiates action to improve or correct the situation.

- Change Management Process

  The change management process aims to plan for and control the risks and impacts of changes to the IT infrastructure. Changes are handled according to standardized procedures to minimize impact on service.

- Release Management Process

The release management process aims to distribute and maintain tested versions of software and licenses for the software. It provides oversight of all other changes and releases to identify any problems or conflicts.

- Knowledge Base Process

  The knowledge base process provides a centralized location for information used in diagnosing and resolving incidents.

- Service Catalog

  The Service Catalog provides links to routine "self-service" functions. Examples include automated password reset, and automated software request.

Step 2: Identify Current Processes

Think about how your organization currently addresses incidents, both formal and informal processes, how incidents are reported, who is the first to find out about them, what happens next, and so on.

Plot the current processes in flow charts, nothing where you would like to see changes. These flowcharts will help guide you when you go into Symantec Workflow to do customization.

Consider these questions when thinking about your current processes:

- Is the process different if the issue is a hardware problem or a software problem?
- Is the process different if you don't know what is causing the issue, only that a user is unhappy?
- How do you determine if an issue is a high priority or what the level of impact to the organization is? This part of the ServiceDesk 7 system is managed by Priority, Urgency, and Impact fields.
- When the root cause is identified, what tools does your team use to troubleshoot and remedy the situation?
- Do you handle incidents differently than problems (based on the ITIL definitions of incidents and problems)? If so, what is the process from start to finish for the Level 2 workers to follow?
- How are service requests handled? For example, if an employee needs to move from one office to another, who in your organization is involved with that and what are the process steps?
- What would you like end-users to be able to do themselves?

Consult your IT staff to determine what part different employees will take in workflows, and how your staff's areas of expertise may influence your ServiceDesk 7 implementation.

Phase 2: Installation, Configuration, and Basic Customization

Installation & Configuration

Notification Server

Before you install ServiceDesk 7, you must install Notification Server and complete at least an initial discovery and inventory. For details, see the Notification Server online help.

ServiceDesk 7

The ServiceDesk 7 installation installs both ServiceDesk and Symantec Workflow Solution.

The ServiceDesk 7 Installation Guide covers all the necessary installation steps and configuration. Configuration includes several important steps, such as determining where users/groups/organizations and permissions come from (typically Active Directory), setting the location of databases, and migrating existing Help Desk 6.5 content.

Migrate Incidents

Migration of incidents can happen during installation or afterwards, from the Service Catalog. Best practice is to migrate all incidents from Help Desk 6.5. Incidents from Help Desk 6.5 are not truly "migrated," rather meta data is brought in; technicians will see the incidents but actually work them in Help Desk 6.5 via an IFrame. Therefore it is necessary to keep Help Desk 6.5 up and running until all of its tickets are closed. Best practice is to cut off users from submitting new incidents into Help Desk 6.5 once incident migration occurs. Since migrated incidents receive their own category in ServiceDesk and are prefixed with "SDM-," you can run a report or sort the list of all incidents to see if the count is down to zero, meaning it is time to take down Help Desk 6.5.

Closed Help Desk 6.5 incidents are automatically imported into the ServiceDesk 7 database for reporting purposes. In fact, you'll notice that closed tickets are not available for migration, since they are already handled behind the scenes. Closed tickets are imported upon the migration, and as tickets are closed post-migration, a ServiceDesk process automatically checks for them once a day and imports those that are found.

Migrate Categories

Migration of categories can happen during installation or afterwards, from the Service Catalog. If you are going to use categories from Help Desk 6.5, best practice is to import them before new incidents are created in ServiceDesk.

Migrate Knowledge Base (KB) Content

Migration of KB content is performed by running a KB Migrator executable found in the Service Catalog. Out of the box, the migrator is configured to migrate Help Desk 6.5 HTML files, however the process can be modified to import content from another document repository. The project that performs the migration is SD.KBMigrationProcess.

Prerequisites:

- Before you run the KB Migrator, you must copy the directory that houses the KB files to the ServiceDesk server. This is required due to .NET restrictions at the command-line level.
- The directory structure for the KB content to copy must follow this format: C:\Libraries*another directory*\Articles. This is the directory structure of HelpDesk 6.5 Knowledge Base content by default. The "another directory" folder represents the individual libraries.
- You must also grant the Network Service account access to the directory

After migration, you can delete the copied directory (unless there were failures and you want to run the migrator again for the .failed content).You can run the migration tool multiple times, however do not run the migrator against content that is already migrated. This is due to high risk of duplication of articles.

Be advised that the migration process takes a long time to complete (testing against the average-sized KB of a few thousand entries took approximately 8 hours). You can check the Configuration Logging Utility for Symantec Workflow to make sure it is still running. (In the tool, right-click the KB migration process, turn on logging, and go to the Log View tab.)

The migration wizard sends notifications throughout the migration process to the e-mail address specified in one of the wizard screens. You are notified each time a KB category successfully migrates, and if there's a failure (down to the specific article that failed).

If a directory fails migration multiple times, you should remove the articles from the source directory, delete the source directory, then try to migrate smaller subsets of those articles to help identify a problematic article. There is a "visual" setting you should turn on in the migration wizard that will provide more detail. The process tries 3 times before it deems a true failure.

Note that the numbering of the migrated articles is new, and is based on the order of import. You could retain your old numbering, however that would also require modifying SD.KBMigrationProcess to get the current number of the article.

After migration is complete, the original source directory can be deleted. Migrated KB articles are stored to the Process Manager database (however images used in articles are saved to the server drive).

Versioning Processes

Before making changes to the Symantec Workflow processes that ship with ServiceDesk, it is important to determine a versioning process. Versioning enables you to return to a prior working state if necessary, and to track the origin of a change.

By default, each time you click Save in Symantec Workflow, a copy of the project is automatically stored in the C:\Program Files\Altiris\Workflow Designer\WorkflowProjects\Backup directory. Up to ten copies are saved.

The versioning method in this section is a very simple versioning method. Its steps include:

1. Create a copy of a project, renaming the copy accordingly
2. Make and test changes
3. Publish to production
    - Use the name of the project (renamed in step 1)
    - Rename the virtual directory (optional)
4. Update the application property in ServiceDesk (optional)

A more sophisticated change management process is detailed in a series of 4 videos posted to http://www.WorkflowSwat.com, under "Learn." This way of maintaining versions of processes is recommended for companies that have larger scale usage of Workflow processes. Symantec recommends reviewing both methods then making a decision that makes sense for your organization.

Pros and Cons of Writing to the Same Virtual Directory

If a process is going to a new virtual directory, you are essentially creating a completely new process (even if the process does the exact same thing as the old process). All of the "in progress" tickets continue to use the original process. ServiceDesk starts to use version 2 of that process for all new instances initiated after publishing AND after updating the application property in ServiceDesk with the new location of the process.

Publishing to the same virtual directory (essentially overwriting an existing process), can break current instances of the process. However, "breaking" is very unlikely for "quick" processes, such as routing rules that only run for a split second.

If you publish over an existing virtual directory the only instances that are broken are ones in an active state. For instance, if you have a web forms process, and people have some forms open, if you publish to that same virtual directory, the next time a button is clicked on the open forms, an error message will display. This is also the case for Workflow processes. If a person is in a Dialog Workflow step and has a form open, the next time a button is clicked, an error message will display. But if a workflow process is at a workflow step and you publish to its virtual directory, nothing is lost since the process was at rest.

The good news is that the process data is not lost when you publish to the same virtual directory. The only information lost was the data being entered into the form at the time.

So when making changes to a project, if the process is going to the same virtual directory, you need to consider the project type. If the process is a Web Forms project type, you do not need to be as concerned about impacting "in process" processes even though you are overwriting the virtual directory contents. This is because Web Forms processes are stateless; these types of projects simply launch when initiated, present the user with a form to fill out, hand off data to another process, and end. They do not have prolonged execution like a Workflow project type that can remain "in process" for an extended period of time, collecting data along the way. However with Workflow projects, more consideration needs to be made, as explained in the following section.

Development Considerations When Publishing to the Same Virtual Directory

An updated URL application property should not break an "in progress" process that uses the old URL. Breaks to processes in this state are more likely caused by changes in the process itself that causes incompatability, such as a piece of missing data.

The way to mitigate incompatibility is to properly build the new version. For instance, say you have a process with two Dialog Workflow components. In the first one, you collect "Name" and "City of Birth" from the user. Then in the second Dialog Workflow component you display this information to a manager.

Now you want to update the process because of a new regulation. Therefore, in the first Dialog Workflow component, you also start collecting "Age." In the second Dialog Workflow component, you add a rule that shows the manager a warning form if the user is 13 or younger. If you simply add this rule, then all submissions that were made before "Age" was collected will be broken. The manager will open his/her task and get an error saying "object reference not set to the instance of an object," because "Age" doesn't exist.

So, to write the new version correctly, you need to add a Variable Exists rule to make sure "Age" exists before hitting the rule that evaluates age compared to 13. If you wrote the second version properly, there should be no risk, since all the instances that were already submitted without age would not break, and all the new instances that were submitted with age would work.

Basic Steps for Versioning

To publish & version a ServiceDesk process in Symantec Workflow (simple versioning method)

1. Create the new version of the project by either copying an existing project, or unpacking the original and renaming it as desired. For example, append a version number to the name, such as "SD.RoutingRules_2_0." Leave the Generate New Service ID checkbox cleared, otherwise the link between the process and ServiceDesk is broken.
2. Modify the project as needed. Make note of the type of the project. Also, decide whether the process will be published to the same virtual directory as the current process. The type of project determines if you need to build in rules to handle new data. The same applies to publishing to the same virtual directory.
3. If it is the first time a project is being deployed, it is necessary to select the Process Manager publishing method, either "Publish to Process Manager Forms" or "Publish to Process Manager Services."
   - If using a new virtual directory, enter the desired directory in the Virtual Directory field. For example, if the old process is in a virtual directory called "SD.RoutingRules," call the new virtual directory "SD.RoutingRules.2.0."
   - The rest of the default settings are acceptable.
   - Select the server where you would like to publish your changes and click OK.
4. From the Application Properties Editor screen, note the new Base URL to Project. Copy this link.
5. Click on Save and complete the publishing process. If prompted, answer the following:

- Open deployed project --> No
- Deploy workflow to NS as DialogWorkflowItem --> No

6. If you changed the name of the project, or if you are using a new virtual directory, to make the new process active in ServiceDesk, it is necessary to repoint ServiceDesk so it uses the updated URL. Log in as Admin and go to the Admin tab > Data > Application Properties.
7. Click on the Actions button (orange lightning bolt) for ServiceDeskSettings and select Edit Profile Definition.
8. Select Edit Settings from the Actions button.
9. Update the appropriate URL field, and click on Save. The application properties take about 45 minutes to propagate.

About Application Properties

ServiceDesk knows which Symantec Workflow processes to invoke based on the URL fields populated from the Admin tab > Data > Application Properties screen. The data in these URL fields, along with several other pieces of information configured here, are called application properties.

Processes "in progress" look to Process Manager for their application properties, (individual processes do not store application properties).

Note:
See the *Process Manager (ServiceDesk) Database* (page 9) section for an explanation of the Process Manager.

Updates made to the application properties are not immediately applied to Process Manager; this is because Process Manager relies on cached application properties. (You can force the new application properties by restarting IIS, thus clearing the cached data, but this is not usually feasible in a production environment.) Once Process Manager updates its cache, then the current processes will start to use the new application properties.

By default, Process Manager updates its cache every 45 minutes, and is set under Admin > Portal > Master Settings > Optimization > Clean Cache Time.

This means that if you update a URL field application property with a new process URL, it does not immediately impact live processes.

Restoring ServiceDesk Processes

ServiceDesk comes with Workflow packages that are unpacked when launched. The original package content is retained, unless a user intentionally overwrites that package. Therefore if you need to revert to the original project, simply unpack the project again.

The Workflow Designer also saves backups of a process upon each save, up to 10. Best practice is to save your changes periodically (i.e., not after every change) in order to have meaningful backup copies. These copies are stored in a Backup directory: Program Files\Altiris\Workflow Designer\WorkflowProjects\Backup.

If you need to obtain the original packages that shipped with ServiceDesk, rerun its installation.

Project Differential Tool

NOTE:
This tool is not yet available in the released version of Symantec Workflow, but should be available in the future.

The Workflow Differential tool takes a baseline project and a secondary project and compares the two, identifying the differences. Use this tool as a first step to identify changes when troubleshooting a project.

The first project selected in the tool is the project to which a second project is compared. Any changes to the following in the second project are identified:

- the libraries the projects utilize,
- Project properties,
- Project resources,
- Project models,
- Components' settings or names.

To open the Project Differential tool in Workflow Solution 7, from the Projects list, select Advanced > Compare Projects. Follow the prompts to select the baseline and secondary projects. If desired, use the import feature to select which changes you want to import into the destination model.

Basic ServiceDesk 7 Customization

Editing the Core ITIL Processes

When you open the core ITIL projects from packages, (for example, SD.IncidentManagement, SD.ChangeManagement, etc.), the process name by default is the file name of the package.

IT IS NECESSARY TO ADD A SPACE in between "IncidentManagement," "ChangeManagement," etc., within the name of the project being unpacked. If you do not add a space, and simply accept the default process name, then you would see two entries for incident management in ServiceDesk, "SD.Incident Management" and "SD.IncidentManagement." (The name of the process shows on the "My Task List" tab, for example.)

Verify Users, Groups, and Organizations

ServiceDesk 7 should automatically read users, groups, and organizations from the Active Directory domain if one was specified during the installation. Log in to ServiceDesk 7 as the administrative user and go to Admin > Users > Accounts > Manage Users page and take a look at the information to see if it appears correct and complete. Administer users,groups, and organziations as needed. Symantec recommends using groups as the primary way of maintaining permissions.

ServiceDesk 7 comes with default groups to which you can add users. (During installation it is possible to map existing AD groups to these default groups.) The groups and associated permissions are defined in the ServiceDesk 7 User Guide.

If native authentication is to be used solely, without Active Directory, it is necessary to add users manually to each respective group.

If you create a new group in ServiceDesk, it is necessary to manually add that group to the application properties in ServiceDesk in order for that group to show up as available data in Symantec Workflow. This step is what makes the new group show up in the profile properties list in Symantec Workflow. (Note: the term "application" is synonymous with "profile" properties in Symantec Workflow.)

To add a new group to the application properties:

1. Create the new group from Admin > Users > List Groups.
2. From the Admin tab, go to Data > Application Properties.
3. Click on the Actions button (orange lightning bolt) for ServiceDeskSettings and select Edit Profile Definition.
4. Click on Next.
5. Scroll down and click on Add Definition Value.
6. In the Name field, enter the name of the new group. For example, "GroupSupportIII."
7. Enter "User Groups" as the category.
8. Leave the data type as text. In the Default Value field, enter "SD.IncidentManagement."
9. Click on Save.
10. Click on Finish.
11. If the new category does not appear in Symantec Workflow (for example, when browsing the profile properties in SD.IncidentManagement), try restarting IIS and reloading the Symantec Workflow project.

Set Up Incident Categories (Classifications)

A good category system is key to building a smoothly running ServiceDesk 7 system. Some of the more useful ServiceDesk 7 reports are sorted by category to help you see what types of issues are most common and what trends are occurring in your environment.

ServiceDesk 7 ships with a list of suggested categories found under Admin > Data > Hierarchy Data Service. (These are the same default categories used in Altiris HelpDesk 6.5.) Change the list as much as you want. Up to 10 category levels can be used. You can also import categories used in Help Desk 6.5 during installation or afterwards, from the Service Catalog.

Remember that the more complex you make the category system, the harder it might be for ServiceDesk 7 workers to correctly categorize incidents. If workers don't categorize incidents correctly, then steps in your processes may be skipped, or the wrong steps processed, or an incident could be routed incorrectly, for example. (The ramifications will depend on the customizations you set up surrounding categorization. Out of the box, categories are simply pieces of information assigned to an incident and no affect is made to workflow.)

Remember that best practice is to not delete a category once you start using it because there is the possibility that an incident is assigned to that category. The incident would

not be removed, rather it retains the old category, and therefore would be left out of reporting and search results if only the new category is used.

Note About Imported Categories

Imported incidents maintain the categorization originally assigned. Imported categories are available for incidents going forward. Imported categories do not map to the default categories in ServiceDesk 7 and therefore some cleanup may be required (i.e., removing categories that seem redundant or not needed).

Verify Default Priority, Impact, and Urgency Values

The Priority, Urgency, and Impact fields of incidents can help you manage Service Level Agreements and comply with the concepts of ITIL service management.

The Priority and Urgency fields indicate how quickly an issue should be resolved. The Impact field indicates how broad an issue is. Impact could be low if just one person is affected, or it could be high if the whole organization is affected.

ServiceDesk 7 ships with the following values for these fields:

- Default priorty values: Emergency, urgent, high, normal, minor, low.
- Default urgency values (on the incident submit form shown to end-users): No Immediate Urgency, Preventing Some Non-Urgent Work, Blocking Critical Business.
- Default impact values (on the incident submit form shown to end users): Single User, Entire Team or Group, Entire Department, Unsure.
- Default urgency values (to technicians): Core business service, Support service, and Non-urgent services.
- Default impact values (to technicians): Department/LOB/Branch, Small group or VIP, and single user.

Note:
You can change the values, however doing so requires caution and a good understanding of the Symantec Workflow software.

The instructions below focus on impact and urgency additions to Incident Management; *if you decide to make priority, impact, and/or urgency changes truly global, so they also apply to Change Management and/or Problem Management, you will need to make many more updates than what is instructed below.* Instructions for updating these processes are contained in the "Editing Priorities in ServiceDesk 7" document, which is available on request from Symantec.

Changing the priority values is likely the most challenging edit, as "emergency, urgent, high, normal," and "low" are hard-coded throughout the Symantec Workflow projects for ServiceDesk, moreso than impact and urgency values. Change priority values only when absolutely necessary.

This example will add "Financial Group" as a new impact, and "No Internet Access" as a new urgency value. **(Please note that "Financial Group" is not a group of users in ServiceDesk, rather a group of employees in a company used as an example.)** First, we will add these values to the form that the end-user uses to submit an incident. Use this example as a model when editing urgency, impact, and priority.

To add new impact and urgency values

1. The technician urgency, impact, and priority values are set as application properties, under Admin > Data > Application Properties. Log in to ServiceDesk as the administrator, and go to Admin > Data > Application Properties.
2. Click on ServiceDeskSettings, in the list of application properties.
3. Click on the Actions button (orange lightning bolt) and select Edit Values.
4. Scroll down to the Urgency, Impact, and Priority category.
5. To add "Financial Group," click on the Add button for Impact.
    - Type "Financial Group" and click on Add. Click on Save.
6. To add "No Internet Access," click on the Add button for Urgency.
    - Type "No Internet Access" and click on Add. Click on Save.
7. Scroll down to the bottom of the the Edit Instance window and click on Save.

Next, it is necessary to update the forms that contain impact and urgency, and then the decisioning made by the process to calculate the corresponding priority.

- If no changes to processes are made, any new urgency value will be treated as a "No Match" in the decision table, and the impact value will equal "Non-Urgent Services."
- If you add a new priority value to the application properties, but don't add that priority value to the decisioning that calculates priority, Incident Management automatically sets the priority to "normal" even if the form selection was the new priority.

To add new impact and urgency values to the end-user Submit Incident form and the decision table that calculates priority

1. Open the SD.Feeder.GeneralIncidentSubmitForm project.
2. In the Primary model, open the Create New Incident Form Builder component.
3. The lower left section of the form contains the Radio Button List components for impact and urgency. Double-click on the radio button component under "Urgecny of this need or issue."
    - In the Items list, add "No Internet Access."
4. Double-click on the radio button component under "Who is Affected?"
    - In the Items list, add "Financial Group." (It will be necessary to expand the size of the Radio Button component box to see the new entry in the form.)
5. Click OK to close the form.
6. Next, double-click the "Show Incident Information, such as Urgency, Impact, User, Needed by Date" Embedded Model component.
7. Open the Set Impact Decision Tree component.
    - Click on Next.
    - Click on Add, and type "Financial Group." This will create the respective entry under the Matches Rule.
    - Click on "Financial Group" under the Matches Rule and in the Urgency field on the right, type "Financial Group."

NOTE:
We are opting to use the same impact value (on the right) that the end-user sees in this exercise, rather than an internal/technician-side value. However the rest of the values under the Matches Rule do use impact values that are technician-facing. (You can see the difference if you click on "Entire Department" under the MatchesRule on the left, for example; notice the corresponding "Department/LOB/Branch" value that appears on the right. Refer back to the bulleted list in the previous section to compare and see the subtle difference.)

- Click on Finish.

8. Open the Set Urgency Decision Tree component.
   - Click on Next.
   - Click on Add, and type "No Internet Access." This will create the respective entry under the Matches Rule.
   - Click on "No Internet Access" under the Matches Rule and in the Urgency field on the right, type "No Internet Access."
   - Click on Finish.
9. Next, we need to set the priority value for the new urgency and impact values; priority is based off the combination of urgency and impact. Double-click the Calculate Priority Decision Table component. Configure as follows:
   - Click on Next.
   - Double-click the Matches Rule for Impact (vertical, on the left).
   - Click on Add. Type "Financial Group" and click OK.
   - Click OK again.
   - Double-click the Matches Rule for Urgency (horizontal, across the top).
   - Add "No Internet Access" in the same manner.
   - Click OK, then OK again.
   - In each "cell" showing invalid, type the desired priority value. It must be exact (no extra spaces). For example, set all of the Financial Group priorities to "High" in all cells except for the cells corresponding to "no match."
   - Click on Finish when complete.

If you changed the priority "Normal:"

1. The priority of "Normal" is hard-coded in the SD.IncidentManagement project > CreateIncidentAdvanced model, in the Set Priority embedded model. Open that model and replace "normal" with the desired value.

Additional Updates for Priority, Urgency, and Impact

You will also want to edit the priority levels hard-coded in the Matches Rule found for SLA calculation, found in SD.DataServices > Setup SLA Requirements.

The goal throughout processes in ServiceDesk is to use the application properties for populating the urgency, impact, and priority values when possible. Occasionally you will come across hard-coded values, for example, in the Matches Rules like you see in the Setup SLA Requirements model.

To make priority, urgency, and impact values truly global, you will also need to update components that have the hard-coded values found in the following projects:

- SD.Feeder.ProbemCreation (there is a decision table for priority in the Create New Problem model > Set Priority embedded model)
- SD.ProblemManagement (there's a Setup SLA model that is inactive by default, but if you choose to customize and use it, be aware there are hard-coded priority, urgency, and impact present)
- SD.ChangeManagement

Verify Close Codes

Close codes in incident management are: Completed Success, Training Required, Review Documentation, No Fault Found, Monitoring Required, Advice Given, Change Required, and Other. If desired, open the SDIncidentManagementProcess project and modify the list. These default values can be changed with no ramifications.

To modify the close code values for Incident Technicians

1. Open the SD.IncidentManagement project in Symantec Workflow. Please see *Editing the Core ITIL Processes* (page 18) if this is the first time opening Incident Managment from its package; there is an important, required step regarding unpacking.
2. In the Initial Diagnosis model, open the Initial Diagnosis Dialog Workflow component.
3. From the Interaction Setup tab, open the Dialog Model.
4. Open the Work/Resolve Incident Form Builder component. This contains the UI technicians access for working an incident.
5. Edit the items list within the Drop Down List component for Close Code to reflect the desired changes.

Portal Master Settings

Portal master settings are established during installation. However, in ServiceDesk, under Admin > Portal > Master Settings, it is recommended to review settings and make basic changes as necessary. At a minimum make yourself familiar with what settings exist. Do not change settings for data like URL, or disable checkboxes without fully understanding the implications; there should be no need to change that type of information.

Examples of basic settings to review:

- Account Management > Password Expire Months setting (default is 6 months)
- Account Management > Register Fail e-mail address
- Account Management > Security Question 1
- Email Settings > Admin Email (change to actual domain admin e-mail address)
- Process Manager Events > these settings determine whether a particular event will automatically generate a message delivered by ServiceDesk (so if users complain about getting prompts within the portal at certain points within a process, you can disable them here; this is different from e-mail notifications which are handled in the Workflow project).

- Report Settings > Process Reporting Interval (sec), makes the information available to web parts quicker (can be dropped to a lower number; makes sense for a smaller-scale SD instance with only a handful of technicians). This setting would work in conjunction with the refresh time of the web part itself.
- Workflow Settings > Task Refresh Time (reduces the default time, in milliseconds, to make a task available to the next user in line)
- Workflow Settings > Auto Refresh Task Page (selected so the user doesn't have to manually refresh the task list)
- Workflow Settings > Task Lease Time (default is 15 minutes, this timeframe can be changed depending on how often you want to check if a lease is broken. This setting comes into play when someone closes a task, since it could be as long as 15 minutes until you find out whether a task is leased or not. Don't lower the time too much; doing so increases overhead on the system.)
- Customization > Logo URL. This adds a company logo in place of the Symantec one in the upper left.
- Process Manager Settings > Update Business Hours (sets the business hours in the portal)
- Process Manager Settings > Help Link URL. Point this to where you have your ServiceDesk documentation housed.

Do not change settings under Application Management, or Process Manager Events.

Determine AD synch method:

- Internal synch method, which is selected by default. Built-in to the PM. Synchs everything. Process Manager Active Directory Settings > AD Sync Process Interval (default is once an hour)
- Workflow method, enabled by checking the Process AD Changes Using Workflow checkbox

Introducing Active Directory Post-Installation

If AD settings were not provided during installation, it is possible to set up AD integration from the Admin > Portal Master Settings screen, under Process Manager Active Directory Settings. Configure these settings accordingly, then add the AD server under Admin > AD Servers page.

The Process AD Changes Using Workflow setting has an upside and a downside to consider: upside is that you can customize the AD Synch process in Workflow so only certain users/groups/organizations synch, therefore getting a better level of control. Downside is that it is more complicated process; it is an interaction of three projects to occur, so you're introducing another element of complexity.

Use the Ignore AD users field to choose not to synch the users listed here.

Customize the General Appearance of the Portal

In ServiceDesk 7, under Admin > Portal > Master Settings, a "Customization" section allows you to set a company logo, pick a theme, menu style, and a few other appearance-related features.

Users with customization permission can further modify their pages. This is discussed further in the setion *Add & Customize Pages* (page 49), and in the ServiceDesk User's Guide.

Customize Form Appearance & Content

In ServiceDesk, the "feeder" screens used to submit data and the pages used to work incidents are built using various form components in Symantec Workflow. Therefore when this document talks about "forms," understand that in terms of ServiceDesk, this means the dialog boxes that appear for entering or working with data that "feed" into the database.

Forms in Symantec Workflow are created using the Form Builder components, often housed within a Dialog Workflow component.

Forms in ServiceDesk are intelligent and enforce validation rules that often had to be manually configured in Help Desk 6.5. These forms enforce required data, enforce the field data type, and can have custom validation set up to further improve the integrity of the data before it is submitted.

In this section, customizing a form entails:

- Setting its appearance using a theme and template,
- Determining the wording on the form,
- Setting the desired closing messages,
- Setting the desired error messages,
- Adding data (additional fields) to forms.

The following sections offer examples to give you ideas of how you can do basic form changes throughout ServiceDesk 7.

Change the Theme and Template for a Form

Themes in Symantec Workflow dictate component control styles (like font attributes), dialog box (form) size, border width and style, and background images. Templates in Symantec Workflow dictate more general features, such as components for pieces of data you want standard across the process (for example, the ticket header information in Incident Management), and the Incident Management logo.

You can modify form appearance by selecting from a range of theme and template styles provided, or create your own.

Note that if you modify a theme or template that came with ServiceDesk, the changes impact all forms that use that theme or template. If a new theme or template is created, it is necessary to manually apply the theme or template to its respective form.

These instructions explain working with themes and templates using the customer service satisfaction survey as an example.

To change the theme and template of the customer service satisfation survey

1. In Symantec Workflow, open the SD.CustomerServiceSurvey project.
2. Double-click the "Customer Service Survey Main Form" Form Builder component. This opens the Web Form Editor.

3. Click the folder icon on the top left. (This is the Select Theme icon.) This opens a Select Theme and Templates window.
    - You can modify the theme listed in the window by clicking the Edit Selected Theme button and making the desired chanages.
    - You can add a new theme by clicking the Edit Project Themes button, then selecting Add to access a blank theme to configure.
    - You can change the theme selection by simply selecting a different theme anc clicking OK (which is necessary when you create a new theme in order to apply it)
    - You can also change the templates by going into the Templates tab on the Select Theme and Templates window. "Service Desk" is the template that the process uses. You can edit this template by selecting the template and clicking on the Edit button on the right.
        - If you want to add a new template, click on New to add a new template, then configure the template.

Note: A form can use more than one template. It depends on how you want to present the data on the form.

To create a new theme using the Composer Theme Editor

1. New themes are created using a utility included with Symantec Workflow. From the Start menu, select > All Programs > Altiris > Workflow Designer > Tools > Composer Theme Editor.
2. Click the New icon to start a new theme. When the theme is saved, it automatically defaults to the directory where themes are browsed to when editing a form. For further information on building themes, consult the Symantec Workflow documentation.
3. New themes will need to be applied manually to the respective forms.

To create a new template

1. New templates are created within the form editor itself by right-clicking the form and selecting Templates > New Template.

Change Task Assingee

In Dialog Workflow components, the Task Assignments tab contains the user/group/organization to whom the task is initially assigned. You can change this assignment as desired by opening up the respective Dialog Workflow component, scrolling down the Task Assignments tab, and updating the Assigments section.

Make Changes to Form Text

This section explains how to make changes to existing text using the customer satisfaction survey as an example.

To change text in the customer service satisfation survey

1. In Symantec Workflow, open the SD.CustomerServiceSurvey project.
2. Double-click the "Customer Service Survey Main Form" Form Builder component. This opens the Web Form Editor.

3. Change the "Thank you" message at the top by double-clicking that component and changing the content of the Text field.
4. Change text style using the options under Look and Feel.
5. To adjust the size of a text field, simply click on the text field in the Web Form Editor and use the mouse to resize. You can also drag and drop existing form fields to reorganize the content.

Note about changing text corresponding with user input
Keep in mind that the output variables for data collected are named to correspond with the default wording of its label. For example, the first customer satisfaction survey question "Ability of ServiceDesk to diagnose your problem?" has a corresponding Radio Button List component to collect the user's input, and this component has an output variable called NewSurvey.QualityOfDiagnosis. If you change the label wording completely, it may be best to rename the variable collecting the output data. This is done by modifying the SD.Data project. Making changes to SD.Data is covered in the section *Extend Data/Profiles* (page 46).

Modify Error Messages

Forms often have required fields; certain data is required by the process in order to continue. Forms in ServiceDesk 7 have error messages built in, however you may want ot modify them. By default, error messages in Service Desk 7 appear only if a required field is not populated. You can get more sophisticated with your error messaging, for example, a specific error message can appear if a field value violates a rule other than the field being empty. (For example, in a numeric field, an error message could say "the value must be between 1 and 10.")

The following instructions use the customer satisfaction survey as an example.

To modify the message that appears when a required field is empty:

1. In Symantec Workflow, open the SD.CustomerServiceSurvey project.
2. Double-click the "Customer Service Survey Main Form" Form Builder component. This opens the Web Form Editor.
3. Within the Form Builder component, find the required field for which you want to edit its error message. (The label shows a red asterisk to indicate it is required.) Double-click the field. For example, double-click the radio button field corresponding to the "Overall quality of the solution?" field.
4. Scroll to the bottom of the Functionality tab. Modify the Required Error Message field as desired. (For example, change "Please answer the Overall Quality question" to "Please let us know how you rate the overall quality, your opinion is important to us.")

Modify Confirmation Pages Presented to End-Users

There are several confirmation pages presented to end-users, such as:

- "Thank you" page upon submitting the customer satisfaction survey with positive results (SD.CustomerServiceSurvey)
- "Thank you" page upon submitting the customer satisfaction survey with negative results (SD.CustomerServiceSurvey)
- Page presented when a ticket is reopened (SD.ReopenIncident)

- "Thank you" page after submitting a Knowledge Base article suggestion (SD.Feeder.KnowledgeBase)
- Login failure form (SD.LoginFailureForm)

Many of these pages are found in the "feeder" Symantec Workflow projects, where information is initially submitted. Most exist as Terminating Form Builder components.

The example to demonstrate this modifies the "thank you" page presented to end-users after submitting an incident.

To modify the confirmation page upon submitting an incident:

1. In Symantec Workflow, open the SD.Feeder.GeneralIncidentSubmitForm project.
2. Double-click the "Thank You" Terminating Form Builder component, found at the bottom of the model. This opens the Web Form Editor.
3. By default, two variables are included in the form content, the incident ID variable and the variable containing the URL to track the incident. You can add more variables as desired by dragging and dropping them onto the Editor screen from the Variables list in the lower left.
4. To edit the text in the form, simply double-click the text component and modify the content of the Text field.

Adding Data to Forms

Adding data to forms requires two steps:

1. Adding the new data to the respective data type, therefore enabling the variable that houses the data to exist. For example, adding CostCenter attribute to the Incident data type.
2. Adding the field to the form so the data can be captured. For example, creating a "cost center" input field for technicians to enter a cost center when submitting an incident.

Step #1 is avery important, more technical, piece. Both of these steps are covered in the section *Extend Data/Profiles* (page 46).

Note about removing data from forms:
Use caution when removing components from a form, as output variables designated by these components will no longer be valid after the removal. For example, if a textbox component gathers data designated as "ReasonforRequest" and it is removed, anywhere in the remainder of the process where "ReasonforRequest" is intended to be pulled and displayed will initiate an error and essentially the process will be broken. A best practice true of any process is to disable components rather than remove.

Additional Form Customization

Additional form customization examples include adding more sophisticated form data validation, marking/unmarking required fields, and setting up custom events surrounding form fields.

An example of custom validation is found in the SD.Feeder.GeneralIncidentSubmtiForm project, in the "Create New Incident" Form Builder component, in the entry field for "Who does this issue affect?" Double-click that textbox component and scroll down to the Validation section to see the custom validation in place. The validation model in this

example makes sure that the submitter isn't the primary contact if submitting for someone else.

By default, ServiceDesk forms enforce required fields for the pieces of information required by the respective process. Requiring a field is as simple as right-clicking the input field and selecting the required path.

ServiceDesk forms can also enforce data format through use of the Masked Edit component. For example, if you add a cost center field or a phone number format to a form, the Masked Edit component enforces that specific format.

For additional information regarding the Forms components, see the Symantec Workflow documentation found on the Altiris documentation site: http://www.altiris.com/Support/Documentation.aspx. (Scroll down to "Workflow.")

Establish Routing (Assignment) of Incidents

Routing rules determine the assignment of an incident. By default, all incidents are routed (in other words, "assigned") to the Support 1 queue. From there, the Support I analyst can re-classify, work, or escalate the incident. Common "routing" rules create assignment based off prioroity, location, and/or category. You can set up multiple layers of rules to determine assignment; the order of the rules is the order in which they are enforced.

Note:
Any time you want to add auto-assignment of incidents to the Incident Management process, simply add the DetermineAssignmentComponent from the ServiceDesk > Data > Incident category of components at the point where you want to introduce a call to that service. By default, a call to this service is done right after an incident is submitted.

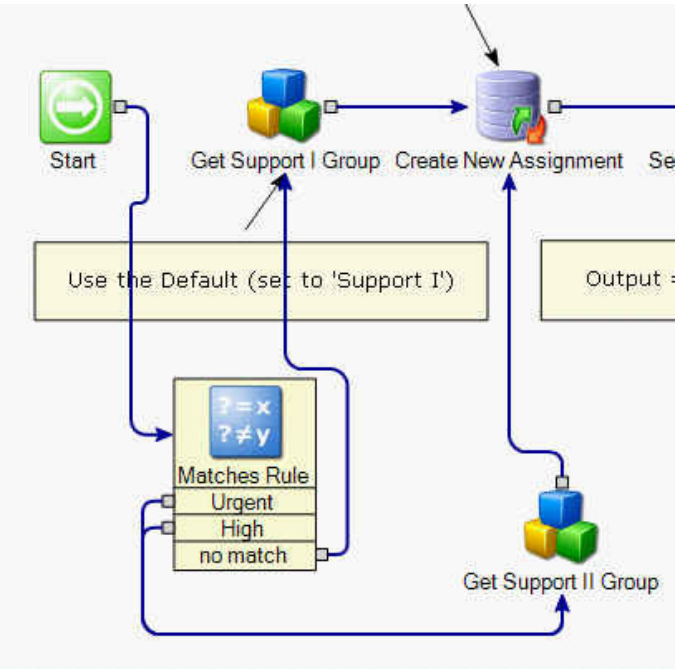
First, let's create a routing rule that will route an incident to the appropriate initial or triage group. This example will show how to have all urgent or high priority incidents automatically routed to Support II.The second set of instructions will show how to route by category, and the third set will show how to route by location.

To create a routing rule to route all urgent or high priority incidents to the Support II group

1. Open the SD.RoutingRules project, and navigate to the Determine Assignment model.
2. Add a Matches Rule, and then copy and paste a replica of the Get Support I component.
3. Configure the Matches Rule so that it finds urgent and high priority incidents by doing the following:
   - Open the Matches Rule. Modify the evaluation list to contain "Urgent" and "High"
   - Set the evaluation variable to be Incident.Priority
   - Click OK.
4. Rename the "Get Support I Group" component to "Get Support II Group"
5. Edit the "Get Support II Group" component to assign as follows:

- Click the "Name" field ellipses button to browse the available data. Pick the property for support II: [[ProfileProperties].service_desk_settings_group_support_ii]

6. Reconnect the project so that it checks for a Support II assignment before the default Support I. If there is an urgent or high incident, the process skips the Support I assignment. If not, it goes to the Support I assignment.



After testing and deploying, incidents in ServiceDesk that are “high” and “urgent” should automatically be assigned to Support II.

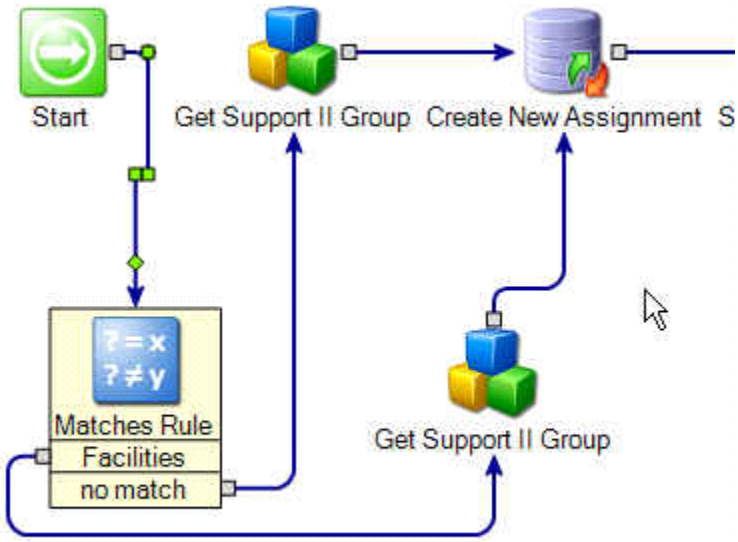
Now suppose when a technician assigns a category, such as Facilities, we would like a routing rule to route the incident to the Facilities group.

These instructions assume “Facilities” exists already as an added top-level category in ServiceDesk, along with the sub-categories: HVAC, Water leak, and Cleanliness Issue. The instructions also assume that the user group “Facilities” exists as well. See the section *Set Up Incident Categories (Classifications)* (page 19) for assistance regarding categories. See the section *Verify Users, Groups, and Organizations* (page 18) for assistance adding groups.

To create a routing rule to route by category

1. Open the SD.RoutingRules project, and navigate to the Determine Escalation model.
2. Add a Matches Rule, and copy and paste a replica of the Get Support II component.
3. Edit the Matches Rule as follows:
   - Type "Facilities" in the Compare To List.
   - Select the variable Incident.Classification_Category_01 as the Compare To Variable.
   - Click OK to close.

4. Rename the "Get Support II Group" to be a "Get Facilities Group"
5. Edit the "Get Facilities Group" component so “Facilities” is the value in the Parameters > Name field on the Input tab.
6. Reconnect the project so that we check for a Facilities assignment before the default Support II



After testing and deploying, incidents in ServiceDesk that are classified as “Facilities” should go to the Facilities group.

Now suppose when a location is provided for an incident, we would like a routing rule to route the incident to a certain group.

The instructions assume that the desired groups exist. See the section *Verify Users, Groups, and Organizations* (page 18) for assistance adding groups. You could set up this example in tandem with the routing by priority example; you could perform priority evaluation first, then route to a special group for “high” or “urgent” incidents for that location, for example.

To create a routing rule to route by location:

1. Open the SD.RoutingRules project, and navigate to the Determine Assignment model.
2. Add a Matches Rule, and copy and paste a replica of the Get Support I component.
3. Edit the Matches Rule as follows:
   - Type the various locations in the Compare To List.
   - Select the variable Incident.Location as the Compare To Variable.
   - Click OK to close.

4. Rename the "Get Support I Group" to the particular group for the first location. Click the "Name" field ellipses button to browse the available data. Pick the property for the respective group.
5. Repeat the replication and configuration of each group, and connect the output paths for each location to the respective group.

Using Reference Data for Routing

There is additional “secondary” data associated with incidents called reference data. It is stored in the dbo.ReportProcessReference table, in the following columns: ReportProcessID (this is the key that links it to the incident), SessionID, ReferenceID, Name, Description, URL, SystemName, ReferenceType. You can take a look at the data in the table to see what each field captures. For example, ReferenceType captures the values “NS Computer,” “Location,” and “Business Service” when any of those are selected for an incident.

Since most customers won’t use reference data, Symantec decided to separate it from the Incident data for simplicity purposes. The following example demonstrates how reference data can be used for routing purposes. A customer has multiple locations, however the location names may change. Therefore, a Site ID is used. A process Reference ID is passed in to a custom database component that does a lookup to match the Reference ID to a site ID.

Note:
This example uses a custom component for querying a custom SQL database table to do a lookup of site ID. This requires an upgraded license for Symantec Worklfow.

To create a routing rule to route by location using reference data

1. Open the SD.RoutingRules project, and navigate to the Determine Assignment model.
2. Add a GetProcessReferences, and add it after the Start component.
3. Edit the GetProcessReferences component as follows:
   - Uncheck the From current process checkbox.
   - Select the variable Incident.ProcessID as the Execution Context ID.
   - Enter IncidentReferences as the Output Variable. (This is an array.)
   - Click OK to close.
4. Add a For Each Element in Collection component following the GetProcessReferences component. Since the incident process references are in a collection it is necessary to use this component to evaluate the data to find the location ID.
5. Edit the For Each Element in Collection component as follows:
   - Select Process References as the Array Variable Type (you may want to search for it for convenience).
   - Select IncidentReferences as the Array Variable Name.
   - Enter SingleReference as the Item Output Variable Name.
6. Next, the process needs to determine what matches up and it’s a text value. Add a Text Equals rule following the For Each Element in Collection component. Connect the Next Element path to the Text Equals component.

7. Configure the Text Equals component as follows:
    - Set the constant value “location” as the Compare Variable.
    - Select SingleReference.ReferenceType as the Variable Name (you may need to check the Show All Data checkbox).
    - Click OK.
8. Connect the Not Equals path of the Text Matches Rule back to the For Each Element in Collection component.
9. Add a custom SQL component to retrieve the Site ID. Pass in the SingleReference.ReferenceID variable as input.
10. Use a Matches Rule to set up routing for the Site ID. (See the preceding instructions for routing by location for an example.)
11. Clone the Get Support I component and select the respective group to which each site will be assigned. Repeat for all the sites desired.
12. Configure the Finished path of the For Each Element in Collection component to handle incidents that don’t have location.

About Auto-Escalation

By default, all auto-escalations due to SLA timeout or resulting from unprivileged escalation, go to Support II. This is determined in the Routing Rules > Determine Escalation model. (Unprivileged escalation means the user does not have the permission to select a particular user or group to whom to escalate; this is the default for all Support I members.)

Allowing Auto-Escalation is a setting configured during installation. However, you can change this setting post-installation from the Admin > Data > Application Properties page.

One example of customized escalation when a ticket times out is to check the user it was assigned to, do search in Active Directory for that user’s manager, then escalate it up to that user’s manager.

About Unprivileged & Privileged Escalation

As described in the previous section, unprivileged escalation means the user does not have the permission to select a particular user or group to whom to escalate. This is the default functionality for Support I. However, you can enable Support I to have privileged escalation capability two ways: by granting the Incident.CanSelectAssignment privilege, or by changing the SD.IncidentEscalation model so the “User Has Permission to Custom Escalate?” component always evaluates true. (Edit the component’s Settings tab > uncheck “Is Enabled” and select true.)

Establish Service Level Agreement (SLA) Times

Incident Management SLA

By default, the SLA timeframes in Incident Management are:

- Basic SLA level:

    - Overall late timespan is 60 days, with a warning at 30 days. You can configure individual levels within this basic SLA. For example, give the Support level 1 8 hours to respond, with a warning at 4. Same with SLA level Support II and "Escalated." Emergency late timespan is 2 hours, with a warning at 1.

- Emergency SLA level:
    - Overall late timespan is 60 days with a warning at 30 days. You can configure it to be more aggresive, for example, overall late timespan of 8 hours, with a warning at 4 hours. Then give the Support level 1 4 hours to respond, with a warning at 2.

The "overall" SLA timeframe is the real SLA requirement the ServiceDesk has to the customer. The levels within the overall SLA are "internal" SLA levels. These internal levels can be looked at as a higher standard that the ServiceDesk holds itself to, to make sure the real SLA ("overall") is never missed.

When the internal SLA level reaches its "warn" time, an e-mail is sent to the current assignee, if it is assigned to a specific user (not a group). The status remains unchanged. When the internal SLA level reaches its "late" time, the status is changed to "OUT OF TIME" and the ticket becomes assigned to Support I and Support II no matter who it was assigned to at the time it hit the "late" time. An e-mail is not sent at this point because the ticket is now assigned to multiple groups of users rather than one particular user.

When a ticket reaches the overall SLA "warn" time, an e-mail is sent to the current assignee, if it is assigned to a specific user (not a group). If the "late" date at the overall level is reached, chances are the ticket already auto-escalated and had notifications sent based on the internal SLAs. Therefore no action is configured in ServiceDesk at this point.

Customers can essentially disable SLAs by increasing the late and warning timespans to a very large number of days if need be. This is recommended if your company is not using SLAs. Currently, ServiceDesk is set up for basic SLA behavior.

Incident Management looks to a global value populated with the SLA status. The workflow components (such as the Dialog Workflow component), in Incident Management use the late date of the current SLA as their timeout value. If a late date is surpassed, the ticket "times out" and takes the time out path out of that component. The incident history is updated to reflect the time out.

Incidents only auto-escalate once by default. This can be changed, as described later in this section.

To change SLA timespans

1. In the SD.DataServices project, open the Setup SLA Requirements model. There are two SLA levels identified, an Emergency SLA level and a Basic SLA level. Within each level is an "Add New Data Element" component that sets the SLA requirements timespans.
2. Open the respective "Add New Data Element" component to edit.
3. Click on the Value ellipses button.
4. At this level, there is a late time span (the time that, when exceeded, denotes the task and the subsequent SLA as late), and a warn time span (the time that, when reached, at initiates a warning that the SLA deadline is approaching). These values will be the overall SLA values, meaning that the levels of approval/action within the

lifespan of the entire process will be within the overall SLA time. Adjust these times as needed.

5. To change the timespans within individual SLA levels, select the respective level and click Edit.
6. Make adjustments to the timespans that make sense for the SLA level, and based on the Set the Late Time Span and Warn Time Spans set at the overall level.

To configure SLAs by customer name, location, contact, or equipment name, etc.

In the SD.DataServices project, open the Setup SLA Requirements model. You want to replicate:

- The component that checks for the piece of information against which the SLA will be applied,
- The Matches Rule,
- The "Add New Data Element" components (or only one, if only one track is desired).

Add the Matches Rule either before the priority level evaluation or after, depending on what is more important to evaluate first. Select the variable to compare against, then connect appropriately. The "no match" path of the component should connect to the original "Add New Data Element" component. Then set the appropriate SLA timeframes for the new SLA.

If you need several SLAs, it may make sense to create new models for each, then use SD.DataServices > Setup SLA Requirements so it makes a call to the appropriate model. Or use a decisioning component to handle which SLA to use.

To enable incidents to time out more than once

1. Open the SD.IncidentManagement project, and navigate to the Set Timeout Date model. Please see *Editing the Core ITIL Processes* (page 18) if this is the first time opening Incident Managment from its package; there is an important, required step regarding unpacking.
2. Copy and paste the "Set Date Far into the Future" End component and place it after the "Has Timed Out Before?" True False Rule component.
3. Connect the true path out of the "Has Timed Out Before?" True False Rule component to the "Add Process Message" component.
4. Connect the "Add Process Message" component to the new End component.

Set Business Hours & Holidays

Business hours and organization holidays can be set at three levels within Symantec Workflow:

- Globally, using the Business Timespan Editor tool (Start > All Programs > Altiris > Workflow Designer > Tools > Business Timespan Editor)
- Project-level
- Component-level, in workflow projects

Determine which level(s) need conifiguration based on your business locations and SLA policy. These levels are for one geographical location. For multiple geographic locations, Symantec recommends getting a consultant's help.

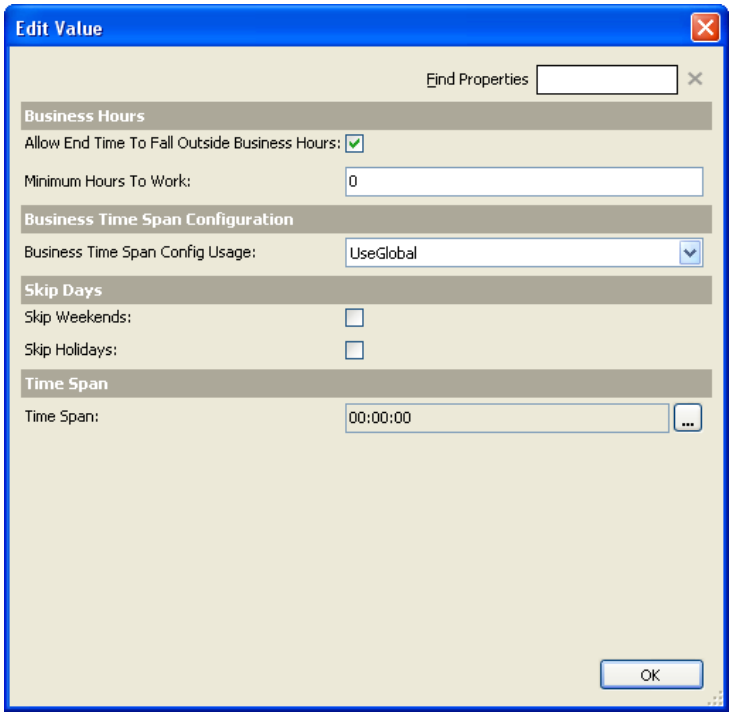
On a global level, business hours and holidays can be set via the Business Time Span Editor, which is one of the tools installed with Workflow Solution and ServiceDesk. These global business hour settings are then picked up and used as the default settings by every new workflow and monitoring project that is created.

The project level represents the second level of business hour and holiday settings. Although initially drawn from the global settings, the business hours can be modified on project-by-project by basis, if necessary. The project level settings can be found on the project attributes screen under the Publishing tab and labeled "Business Time Span Config." The ability to incorporate business hours respective to individual projects may be beneficial, for example, if an organization has a department that operates through the weekend while the majority of other departments operate only during the business week. The retail industry would be a prime example of this.

Finally, business hours can be further customized at the component level (within workflow projects only).

On their own, the business hour settings do not affect the way a workflow project is executed. But when appropriate they may be incorporated at the component level to allow or prevent certain actions from occurring based on established business hours. A very common example is the consideration of weekends and holidays when establishing timeout and escalation rules, and in the Emergency track of the default SLA.

Below you see a screenshot taken during configuration of a Dialog Workflow component. The dialog box pictured is used to set up the proper timeout and escalation schedules for this activity.



There are four settings which look to the business hours to ensure proper execution:

- Allow End Time To Fall Outside Business Hours
- Skip Weekends

- Skip Holidays
- Business Time Span Config Usage

Using “Allow End Time To Fall Outside Business Hours” establishes that a process can auto-escalate or timeout between workdays even if the critical time threshold is reached outside of normal business hours (i.e. for most businesses this effectively means that an activity can escalate or timeout overnight). “Skip Weekends” and “Skip Holidays” ensures that only business days are counted in the escalation/timeout process.

Finally, the drop-down box labeled "Business Time Span Config Usage:" is used to specify whether the component should look to the global business hour settings, the project settings, or the custom settings on this component itself.

Set Up “Follow the Sun”

The SD.FollowTheSun project is where groups to assign to an incident are defined when the incident is marked to “follow the sun.” In the primary model of this project, it is necessary to:

- Verify/change the default time of day evaluation (set in increments of six hours by default)
- Establish location names that would cause an incident to move for each time range (edit the “Build List of Locations to Move” Add New Data Element components)
- Establish group assignment for each location (edit the “Build List of New Group Assignments” Add Items to Collection components)
- Verify/change the value of the “Set New Task Duration in Hours” Add New Data Element component (default value is six hours)

Each of these items to configure is pointed out within the model.

Change the Frequency of the Customer Service Satisfaction Survey

In Service Desk, a task is assigned to the customer after his/her incident is resolved. He/she has the option to either reopen the issue or resolve it.

On picking the “Issue Resolved” path in the Confirm Incident Resolved form, the process hits the Random Rule component.

By default, this Random Rule component is set to 100, meaning the customer satisfaction survey is sent after every incident is confirmed as resolved by an end-user.

Service Desk may not always want to send a survey to a customer every time his/her ticket is resolved. Any process that sends out a survey form to the customer can be modified in such a way that it sends out surveys only for a particular percentage of time. For example, a process can be set up to send surveys for 30% of the time. This means that out of the 10 tickets resolved, only 3 customers (assuming the 10 tickets are submitted by 10 different customers) get the survey. The random rule would be set to 30 in this case.

To disable the survey entirely, set the Random Rule to zero, or disable the Random Rule component and set its execution outcome to “false.”

To configure the Random Rule component

1. Open the SD.IncidentManagement project in Symantec Workflow. Please see *Editing the Core ITIL Processes* (page 18) if this is the first time opening Incident Managment from its package; there is an important, required step regarding unpacking.
2. In the Projects list on the left, click on the Customer Confirm Resolution model.
3. Double-click the "Have Customer Confirm Resolution" Dialog Workflow component to edit it.
4. Select the Interaction Setup tab.
5. Double-click the Random Rule component that follows the "Confirm Incident Resolved" Form Builder component.
6. Click on the ellipse in front of True Percentage. Type the desired constant value. Or, instead of using a constant value for the True Percentage variable, you can use process variables or a dynamic model.

You can use different rules in your process for sending out the customer survey in place of the Random Rule component as desired. For example, if the incident is of a certain type or priority, then always send the survey. You could set up this type of rule using Matches Rule or a Decision Table component.

Define Quick Incident Templates

A ServiceDesk 7 feature that speeds up the processing of incidents is Quick Incident Templates. Quick Incidents templates are pre-populated incident submission templates that have pre-defined, standard values for common issues. For example, server reboots or password resets are frequently requested in most organizations, and there are many values in these incidents that are set the same way every time. Instead of the ServiceDesk 7 worker setting all of these values manually every time a password is reset, the worker can select a Quick Incident Template for password reset and all of the fields in the incident will be set to the proper values. Set up as many different quick incidents as you need, and they can be modified at any time based upon the changes that occur within your environment.

Quick Incident Templates can be specific to a user, group, or organization, or shared globally. End-users do not use quick incident templates, rather technicians through the "Advanced" incident submission process.

You can also create quick incident for sub-tasks.

To create a quick incident template

1. In ServiceDesk, from the Service Catalog, select "Submit Incident (Advanced)."
2. Populate the form with the information that will be standard and give it a name and description.
3. Click the Save As Template button.
4. Enter the template name, then decide if it's user-specific or to be shared. If it's shared, set the appropriate permissions. The next time an incident is created using the "Advanced" form, it is possible for the user(s) with permission to select the template from the "Select Template" drop-down menu.

Define E-mail Content

E-mail content is handled in two ways in ServiceDesk. Sometimes the content is actually housed in a Send Email component within a process. But more often than not, processes in ServiceDesk make a call to the SD.EmailServices application to generate an e-mail.

E-mail templates are stored in the SD.EmailServices project. Think of a template as a definition of the content within an e-mail message.

This section covers both editing directly in the Send Email component and in the template within the SD.EmailServices project.

To modify the customer confirmation e-mail (Send Email component)

1. Open the SD.IncidentManagement project in Symantec Workflow. Please see *Editing the Core ITIL Processes* (page 18) if this is the first time opening Incident Managment from its package; there is an important, required step regarding unpacking.
2. In the Projects list on the left, click on the Customer Confirm Resolution model.
3. Double-click the "Have Customer Confirm Resolution" Dialog Workflow component to edit it.
4. Click the Event Configuration tab and click the ellipse next to Start Process.
5. Double-click the Thank You Subject Merge Text component, or the Thank You Body Merge HTML component.
6. On the Configuration tab, click the ellipse next to Merge Data.
7. In the Advanced Text Creator window, add, modify, or delete text as appropriate.

To customize the global header and footer for e-mails

1. Open the SD.DataServices project in Symantec Workflow.
2. Scroll down to the bottom of the models list, and open the GetEmailTemplateParts model.
3. Configure the "Build Email Header" and "Build Email Footer" components as desired. You can add a project property for a logo, then populate these components with that property to have a corporate logo appear.

To add a new e-mail template

1. Open the SD.EmailServices project in Symantec Workflow. Notice that existing templates, named according to the content, only have components for the subject line, body, and header.
2. Add a new model, selecting the parent model as the respective category where the e-mail template will be used (ex: IncidentTemplates). Use a naming convention that reflects its function. It is required to use the appropriate prefix to the model name in order for that template to automatically be available; for example, Incident.XYZTemplate for a template in Incident Management.
3. Copy and paste the components from an existing template as a shortcut. Or, manually add a Merge Text component for the subject line and configure.
   - Use a Merge HTML component for the body of the e-mail and configure.
   - Use a Merge Text component for the header and configure.

To modify an e-mail template

1. Within the SD.EmailServices project in Symantec Workflow, review the subject, body, and header for the existing e-mails sent. Particularly pay attention to the ones interfacing with end-users.
2. Modify text as needed, in addition to adding variables to include more data if needed.

Note About How the E-mail Templates are Selected in ServiceDesk

When called, the e-mail services application either automatically uses a template based on parameters passed in, or proceeds in a "generic" fashion that makes it possible for the technician to select a template.

E-mail services first looks for ProcessID and TrackingID variables and if either of those are found, it acquires the corresponding data. The templates made available at this point will be specific to the type of project that corresponds with the process ID. (For example, if the process ID is IM-000001, then the list of templates will be from Incident Management.)

If no process ID or tracking ID are found, the service presents the user with a basic e-mail form that requires manual population of data.

Customize E-mail Monitoring

ServiceDesk 7 can accept new incidents or updates to current incidents through the inbound e-mail interface. The e-mail process is found in the SD.Email.Monitor project.

The e-mail address, user name, password, e-mail type, and server information is all set up during the installation process. (Changes can be made however from the Admin tab > Data > Application Properties.)

Brief Overview of How it Works & Ideas for Customization

The SD.Email.Monitor process allows for anyone to send in an incident using a standard e-mail. If the subject line includes the words "New Incident" or "New Ticket," the e-mail monitoring process automatically creates a new incident and sends the mailer a return e-mail that an incident was created. You can add additional words to look for that would qualify the creation of a new ticket, or additional rules.

You can also set up monitoring to look for strange characters to do additional spam filtering if unwanted e-mails are making it into the ServiceDesk Inbox.

To set up additional words acceptable as subject text:

1. Open the SD.Email.Monitor project in Symantec Workflow.
2. Click on the ProcessMessage model in the Project tree.
3. Double-click the "Is New Incident Request?" Embedded Model component.
4. Copy and paste the existing "Looking for New Incident:" Text Contains Rule component. This component will follow the "does not contain" output path of the "Looking for New Ticket:" Text Contains Rule component.
5. Connect the "contains" path to the "New Incident" End component.

6. Connect the "does not contain" path to the "Not New Incident" End component.
7. You can also change the existing "New Ticket" and "New Incident" text as desired.

If the e-mail does not contain the words "New Incident" in the subject line, a task is created for the Service Managers (this is done in the SD.Email.InboundManagement project) to review the data and classify it as either an incident, problem, change, or knowledge base request. The assignee for this task can be customized in the SD.Email.InboundManagement project.

The system identifies the user based on the "From" address. If the user is not listed as a contact, it can be automatically added, and an incident is created based upon information contained in the e-mail. The e-mail subject line becomes the title for the incident, and default values, such as queue, status, urgency and the like are assigned.

It is possible to use an incident rule to parse the body of the message looking for specific words or phrases, such as "windows," "Word," "Excel," "printer," or "corporate headquarters." If specific words or phrases are identified, then specific ticket types or field values can be set within the incident.

The E-mail process relies on an automatically-generated reply code to link e-mail correspondence to an incident. (E-mail correspondence becomes a part of the incident history; it is not necessary for a technician to check an Inbox.) If a reply code is deleted for whatever reason, the Service Manager by default gets a task to review the e-mail and can associate it to an existing ticket.

Processing Large Amounts of E-mail

The SD.Email.Monitoring process allows for quick processing of e-mails, however if you tend to have a large bulk of e-mails to process, it is recommended to modify the e-mail monitoring process to change it to a Windows Service.

To set up e-mail monitoring as a Windows Service

1. Open the SD.Email.Monitor process in Symantec Workflow.
2. Click on the main model in the Project tree.
3. Click on the Publishing tab, and change the deployment type under Deployment to Windows Service.
4. Publish the project as an Installer.
5. Copy the installer file to the server.
6. Execute the installer.

Implement Multiple Mailbox Monitoring

The SD.Email.Monitor process is set up to watch or monitor a single mailbox for inbound e-mail. The process can be modified should your organization utilize multiple mailboxes that each serve a particular role/function for e-mail collection.

The easiest way to implement multiple mailbox monitoring, however, is to set routing up on the mail server-side so e-mails go to the monitored inbox. But if you want to do it using Symantec Workflow, follow the instructions in this section.

To set up a second e-mail box to monitor (high-level steps)

1. Open the SD.Email.Monitor process in Symantec Workflow.

2. Update each mail component to reflect the additional inbox/mail server.
3. Publish the new process, but rename the virtual directory. For example, SD.Email.Monitoring.Server2.

Modify the Timespan for End-Users to Confirm Incident Resolution

By default, end-users are given two days to provide confirmation of incident resolution; "confirmation" means either answering that the incident is resolved satifactorily, or reopening the incident. The incident will remain at 90% complete, and therefore open, until it is resolved with end-user satisfaction. The two-day duration can be modified.

To modify the timespan for incident resolution

1. Open the SD.IncidentManagement project in Symantec Workflow. Please see *Editing the Core ITIL Processes* (page 18) if this is the first time opening Incident Managment from its package; there is an important, required step regarding unpacking.
2. In the Projects list on the left, click on the Customer Confirm Resolution model.
3. Double-click the "Have Customer Confirm Resolution" Dialog Workflow component to edit it.
4. Click on the Even Configuration tab, and scroll to the Timeout Configuration section at the bottom.
5. Click the ellipse next to Timeout Time Span.
6. Change the value from two days to the desired duration.

Add a Cube Report Schedule

A cube report schedule is required in order for cube reports to show data; these reports will be initially blank otherwise. Cube report data is only as current as the last update performed as dictated by the schedule.

To create a cube schedule

1. Log in to ServiceDesk as the administrator. From the Admin tab, go to > Reports > Cube Schedule List.
2. Click on the Add Cube Schedule icon (plus sign) on the right.
3. Configure the cube schedule. Some important definitions:
   - Process full - Process everything, regardless (runs all report data)
   - Unprocess - Remove all data from the cube
   - Process default - Only process cubes that are modified

You can get very granular on which data to update in a specific cube. For example, you can configure the cube to update a high priority incident count every minute but have the rest of the cube update every 10.

Establish Change Management Groups

If Change Management is to be used, the user groups associated with it, such as the CAB, need to be defined in ServiceDesk. Modify the default groups to include the appropriate individuals responsible for handling change. This is done from the Admin tab, under > Users > Accounts > List Groups. Create change groups as needed and add the respective users. Be sure to name the groups prefixed with "Change-" otherwise the change templates cannot pull in that group. For example, "Change Team-Nofolk."

NOTE: If the new groups do not show up in the respective form in ServiceDesk, restart IIS.

Change Risk Assessment Participation for Change Management

By default, 100% of participants at each step in the ITIL change type must approve/ participate in order for a change to occur. You can modify this so that a change proceeds after just one person approves, after a specific user name approves, or after a majority approves. This example shows how to modify the process so it proceeds after one member of the CAB provides risk assessment.

To modify the risk assessment task so when one risk assessor completes the task, the Change process moves forward

1. Open the SD.ChangeManagement project.
2. Go to the Risk Assessment model.
3. Zoom out to find the Risk and Impact Assessment Dialog Workflow component.
4. Change the connection from the 10% Risk Assessment component so it connects to the Risk and Impact Assessment Dialog Workflow component, rather than the Iterate Risk Assessors component.
5. Instead of deleting the Iterate Risk Assessors and the Loop Back components, opt to disable them as follows:
   - Double-click the Iterate Risk Assessors component.
   - From the Settings tab, clear Is Enabled and select finished as the Execution Outcome. The finished path must connect to the Wait for All Workflow Components (Merge) component.
   - Click OK.
   - Double-click the Loop Back component.
   - From the Settings tab, clear Is Enabled.
   - Click OK.
6. Double-click the Risk and Impact Assessment Dialog Workflow component. Configure as follows:
   - From the Assignments tab, click the Person Assignments field Browse button.
     - Click AllParticipantsRow.EmailAddress and click Remove.
     - Click Add > From Process.
     - Click Pick Array.
     - Select RiskAssessors[ ] > [*]> EmailAddress and click OK. (The Variable name field below shows RiskAssessors[*].EmailAddress.)

        - Click OK, then OK again.
    - Click OK to close the Variable Assignments screen.
    - Click the Interaction Setup tab.
    - Click the Dialog Model field Browse button.
        - Scroll right and double-click the Rename Risk Assessment Doc File Name component (This is a renamed Merge Text component).
        - Click the Merge Data field Browse button.
        - Click AllParticipantsRow.ParticipantName and press the Delete key.
        - From the Data tab on the left, expand EnsembleSecurityToken and then select Name.
        - Drag and drop EnsembleSecurityToken.Name in the previous location of AllParticipantsRow.ParticipantName.
        - Click OK, then OK again.
    - Click OK to close the Edit Embedded Decision Model screen.
    - Click OK to close the Risk and Impact Assessment Editor.
7. Double-click the Wait for All Workflow Components (Merge) component. Configure as follows:
    - Click the Data Merge Model field Browse button.
    - Right-click the Merge Impact Risk Assessment Merge Data component and select Copy.
    - Click OK to close the submodel.
    - Click the Settings tab.
    - At the bottom, clear Is Enabled and select done as the Execution Outcome.
    - Click OK.
8. Right-click the bottom of the Designer screen and select Paste to paste the copied Merge Impact Risk Assessment Merge Data component.
9. Connect the copied Merge Impact Risk Assessment Merge Data component to the End component.
10. Connect the timed out path of the Risk and Impact Assessment Dialog Workflow component to the copied Merge Impact Risk Assessment Merge Data component.
11. Connect the Add Process Message component at the bottom of the Designer screen (the one following the default output path from the Risk and Impact Assessment Dialog Workflow component), to the copied Merge Impact Risk Assessment Merge Data component.
12. Double-click the copied Merge Impact Risk Assessment Merge Data component. Configure as follows:

- Click the Merge Data field Browse button.
    - Delete the AllParticipantsRow.ParticipantName data from the editor screen.
    - From the Data tab on the left, expand EnsembleSecurityToken and then select Name.

- Drag and drop EnsembleSecurityToken.Name in the previous location of AllParticipantsRow.ParticipantName.
- Delete the piece of previous data for the risk score.
- From the Data tab on the left, drag and drop RiskScore in the location of the previous risk score.
- Delete the piece of previous data for the risk assessment.
- From the Data tab on the left, drag and drop ImpactAndRiskAssessment in the location of the previous risk assessment.
- Click OK, then OK again.

13. Click Save.

Verify Problem Categories

Just as you can update Incident resolution codes without ramification, you can do the same with problem categories. The default categories are: Add - Install, Break - Fix, Request.

To change problem categories

1. Open the SD.ProblemManagement project.
2. Go to the Problem Analysis model > Problem Analysis Dialog Workflow component > Interaction Setup > Dialog Model > Verify Problem Form Builder component.
3. Double-click the drop-down list component that houses the categories.
4. Update the list of values as desired.

Phase 3: Advanced Customization

Extend Data/Profiles

About SD.Data

The integration library SD.Data exposes data types in ServiceDesk that are meant to be modified. This library is meant to be used particularly for the introduction of new data. There is another library that houses the core data types in ServiceDesk. This core library is intentionally inaccessible by users for protection purposes. Therefore Symantec exposed SD.Data for users to change without jeopardizing the core data types, thus protecting the integrity and functionality of ServiceDesk.

Extend the ServiceDesk Incident Data Type

The ServiceDesk Incident data type is the central and unifying element within Incident Management. This data type is predefined to include properties relative to working incidents, such as name, description, closure code, impact, SLA, etc. Your organization may require the inclusion of specific properties to better refine how your incidents are handled.

Add Cost Center to Incident Data Type

The example that follows demonstrates the addition of the data "cost center" to the Incident data type so technicians can enter a cost center value when creating an incident. First the data will be created, then the form for submitting an incident will be modified to collect the cost center. (Note that Cost Center is just used arbitrarily as an example; since this is a value in the NS, it is likely true cost center would come from that source.)

To add cost center to the incident data type

1. In Symantec Workflow, open the SD.Data integration library.
2. Select the Advanced option at the bottom of the window then Edit Advanced Settings.
3. Select Edit Included Assemblies.
4. Browse the Included Assemblies path and insure that the following path has been selected, (for the respective disk drive): C:\Program Files (x86)\Altiris\Workflow Designer\WorkflowProjects\SD.Data\libs
5. Select SD.DataTypesCore.dll, Select Open, then OK.
6. Select OK to exit the Dynamic Type Editor Form.
7. Return to the SD.Data section of the Integration Library screen and click on Adjust Definitions.
8. In the Generators Management window, expand Generators then double-click SD.Data. The Generate Components wizard will open.
9. Highlight ServiceDesk Incident and click on Add Property.

10. The Edit Property window will open. Type a name for the property then select the property Type from the drop-down list. For example, name the property "CostCode" and set its data type to Number (integer).
11. Add as many new properties as needed, and then click Next in the wizard.
12. Click within the Name column for each added index, and rename the property accordingly.
13. Click Next on the Indexes screen and Next again to move past the Settings section.
14. In the Components section, click Finish.
15. In the Integration Library window, click Recompile and Close.

The new attribute of the Incident data type should now be available. (It may be necessary to reload any open projects if the data type is not showing up.)

Add Cost Center to Incident Form

To add a cost center field to the Submit Incident (Advanced) form

1. In Symantec Workflow, open the SD.Feeder.GeneralIncidentSubmitForm project.
2. If the new attribute was just added, a prompt will appear asking to overwrite the local library with the server version. Leave the checkboxes unchecked to keep the local library. Click OK.
3. Right-click the "Create New Incident" Form Builder component and select Web Form Editor.
4. Resize the text box for the incident description to make room for the new field.
5. From the Variables pane in the lower left, expand Incident and scroll down to find CostCode.
6. Drag CostCode to the space made available in the form.
7. Choose the most suitable builder option, which in this example is InputBuilder (Decimal).
8. Click on Next.
9. Choose the appropriate output paths. In this example, make the CostCode value optional for users choosing Continue and ignore it for everything else.
10. Double-click the Cost Code label to edit it, then click OK.
11. Resize and reposition the field if necessary.
12. Click OK to close the form editor.

Using Custom Data in Reporting

Custom data will appear as an available field in reporting only after that piece of data has been used (i.e., populated) once.

Use Custom Data in Process View Page

This step is necessary if you want users to be able to show a new custom value in the Process View page.

To enable users to display custom data on a Process View Page

1. Log in to ServiceDesk as the administrator.
2. Go to the Admin tab > Data > Lists/Profiles
3. For Incident Management, select Edit Profile Definition
4. Place a checkmark next to the new field. Note: SQL likely renamed the new field based on uppercase letters to lower-case.
5. Click on Generate.

Extend the CustomerServiceSurvey Data Type

The customer satisfaction survey is meant to be modified by customers to reflect what is important to the organization.

ServiceDesk has a data type for the customer satisfaction survey, called CustomerSerivceSurvey. This data type also resides in the SD.Data integration library. If you want to add a question to the survey, it is required to add the attribute for that question to the CustomerServiceSurvey data type.

Then, add a field for the new attribute in the survey itself. The survey is found in the SD.CustomerServiceSurvey project, in the "Customer Service Survey Main Form" Form Builder component.

One idea for customization is to add comment fields for each question, rather than having one general comments field at the end of the survey. For example, capture a specific comment for a specific question if the rating for that question is less than 3.

Follow the procedures in the preceding section "Extending the ServiceDesk Incident Data Type," but make adjustments appropriate for the customer satisfaction survey.

Extend the Change Request Data Type

The ChangeRequest data type is the central and unifying element within Change Management. This data type is predefined to include properties relative to implementing changes, such as name, description, schedule, impact, duration, etc. Your organization may require the inclusion of specific properties to better refine how your changes are handled.

Add new attributes as needed to the ChangeRequest data type in the SD.Data project.

Follow the procedures in the preceding section "Extending the ServiceDesk Incident Data Type," but make adjustments appropriate for Change Management.

Extend the ServiceDesk Problem Data Type

Modifications in the ProblemTicket Data Type

A data type can be thought of as a constraint placed upon the interpretation of data in a process. ProblemTicket data type is the data type we associate with any problem in the Problem Management process. The data type is associated with properties such as title, urgency, description, SLA, etc. These properties move around in the process with the data type.

Add new attributes as needed to the ProblemTicket data type in the SD.Data project.

Follow the procedures in the preceding section "Extending the ServiceDesk Incident Data Type," but make adjustments appropriate for Problem Management.

Add & Customize Pages

Pages in ServiceDesk can be added as needed to make additional data available to users. Also, pages can be customized. The goal is to make information available and presented in a way that makes handling tickets quick and effective. Examples of customization include:

- Adding new web parts to pages (See the following section *Create a Web Part* (page 60))
- Reorganizing existing web parts
- Creating Process View pages for handling incidents (for example, a different Process View page for a change ticket vs. a ticket in Incident Management)

Pages are created under Admin > Portal > Manage Pages.

Users with page customization permission can edit their pages from the Site Actions menu. Admins can edit pages from the Admin > Portal > Manage Pages page.

There are well over a hundred web parts in ServiceDesk; many of them are categorized under Admin > Portal > Web Parts Catalog. Additional web parts are available by clicking the Add icon on that page and making a selection from the Class Name drop-down menu. That is the full list of web parts available.

Plugins can be added in ServiceDesk as well under Admin > Portal > Plugin Upload.

Modify Types of Changes

Within the Change Management main model, SD.ChangeManagement, a form provides the type of change for a proposed change request. If your organization only utilizes a few of the change types, you may want to modify the Type of Change form and outgoing paths. The default types of changes available are: ITIL, Moderate, Simple, and Emergency.

You have two options. You can delete the components for the one(s) you don't want, or you can have the component always utilize one change type.

To remove types of changes

1. In Symantec Workflow, open the SD.ChangeManagement project. Please see *Editing the Core ITIL Processes* (page 18) if this is the first time opening Change Managment from its package; there is an important, required step regarding unpacking.
2. In the Change Management Main model, double-click the "CM (Gatekeeper)" Dialog Workflow component.
3. On the Interaction Setup tab, open the Dialog Model.
4. Double-click the "Type of Change" Form Builder component.
5. In the Web Form Editor, select the specific components to remove then click Delete.
6. Click OK to close the form when editing is complete.

7. Immediately following the "Type of Change" Form Builder component are Add New Data Type components for each change type. Note the Add New Data Type component with the validation break (since its type of change was removed).
8. Delete the errant component (or if there is a possibility it will be needed in the future, double-click the component, go to its Settings tab, and uncheck the "Is Enabled" checkbox).
9. Delete the change type option from the Matches Rule.

Note: You may want to remove the entire change type section from the embedded decision model however, it should be noted that if the related components are not removed but the initial entry into the path was deleted, there will be no risk that the process will migrate to that area of the workflow.

To enforce one type of change

1. In Symantec Workflow, open the SD.ChangeManagement project. Please see *Editing the Core ITIL Processes* (page 18) if this is the first time opening Change Managment from its package; there is an important, required step regarding unpacking.
2. In the Change Management Main model, double-click the "CM (Gatekeeper)" Dialog Workflow component.
3. On the Interaction Setup tab, open the Dialog Model.
4. Right-click the "Type of Change" Form Builder component and select "Edit Component."
5. Click on the Settings tab.
6. Uncheck the "Is Enabled" checkbox.
7. From the Execution Outcome drop-down menu that appears, select the desired change type. This means the component will always use this type of change as its outcome, as if the user selected it.
8. Click OK to close the component. The component will appear inactive, however it will function by setting the execution outcome therefore causing the process to follow the respective path.

Define Smart Tasks

Smart Tasks are tools that ServiceDesk 7 workers can use to help work a ticket. These tools can execute a program, invoke a web service, trigger a task server job, or call a web page, for example. Here are some examples of ways to use Smart Tasks:

- Run the resource association diagram to see how the computers are logically set up.
- Show a list of in-stock computers.
- List all incidents associated with a specific asset.
- Send a request for approval.
- Search the Altiris Knowledge Base web site.

Add Smart Tasks to the Initial Diagnosis Dialog Workflow

Create smart tasks for actions that are performed often. There is no limit to the amount of smart tasks you can add to Incident Management; conceivably, each will expand your ability to work an incident.

This example will create a smart task for automatically searching the Altiris Knowledge Base using the ticket's description.

To create a smart task for searching the Altiris Knowledge Base web site

1. In Symantec Workflow, open the SD.IncidentManagement project. Please see *Editing the Core ITIL Processes* (page 18) if this is the first time opening Incident Managment from its package; there is an important, required step regarding unpacking.
2. Within the Main Incident Work model, double-click the "Diagnose and Work Incident" Linked Model component.
3. Double-click the "Initial Diagnosis" Dialog Workflow component.
4. Select the Interaction Setup tab. The existing smart tasks will be listed as dialog models.
5. Click Add.
6. From the Setup tab, set the Category as "Tools" and provide a name for the new smart task. In this example, the name is "Search Altiris KB."
7. Open the Dialog Model. This is where the process itself is configured.
8. Add a Merge Text component to the new dialog model and double-click the component to edit it.
9. Open the Merge Data model. It is easiest to paste in the URL of the Altiris KB rather than type it, therefore go to the Altiris KB site: http://kb.altiris.com. (Leave the Merge Text component open.)
10. Do a simple search, for example, type "test" in the Search Terms field then click on Search.
11. On the right, under Last Searches, right-click the "test" link and copy the URL to the clipboard.
12. Back in Symantec Workflow, in the Advanced Text Creator window of the Merge Text component, paste or type the URL of the site.
13. Where the URL has "test," delete "test" and add the variable for incident name. This is done by dragging and dropping the Incident.IncidentName variable from the Data tab on the left into its respective position within the string.
14. Click OK and provide an output variable name. For this example, we will use "AltirisKBURL."
15. Click OK, and back in the Decision Model editor, add a Terminate and Transfer Dialog Flow component.
16. Double-click the component, and in the URL field, select Process Variables, then Add.
17. Select the output variable name that you created in the Merge Data component, in this example, "AltirisKBURL." Click OK.

18. Connect all of the components together.
19. Click OK three times to exit the component editors. The new smart task will be applied the next time you deploy the process.

NOTE:
Smart tasks may or may not complete the task to which they are associated. If the checkbox "Resolve Workflow Task on Exit" is selected, the smart task would resolve the task. If the checkbox is left unchecked, the smart task can be run as many times and the task would remain unresolved.

It is possible to configure smart tasks to appear conditionally, so they only appear when it makes sense. This example will demonstrate how to configure the "Search Altiris KB" smart task created in the preceding steps so it only appears when the ticket name contains the word "Altiris."

Additionally, a date range can be specified for making the smart task available by using the "Date Validity" setting for the smart task.

To enable smart tasks to appear conditionally

1. In Symantec Workflow, open the SD.IncidentManagement project. Please see *Editing the Core ITIL Processes* (page 18) if this is the first time opening Incident Managment from its package; there is an important, required step regarding unpacking.
2. Within the Main Incident Work model, double-click the "Diagnose and Work Incident" Linked Model component.
3. Double-click the "Initial Diagnosis" Dialog Workflow component.
4. Select the Interaction Setup tab.
5. Click on the Search Altiris KB smart task and click on Edit.
6. From the Setup tab, check the "Conditionally Use" checkbox.
7. Open the Conditional Use Model. For this mdoel, only the Text Contains Rule component is needed to evaluate the incident name for the word "Altiris."
8. Add a Text Contains Rule component to the model.
9. Since the Text Contains Rule component has two outcomes, another End component is needed. Add an End component.
10. Connect the components accordingly.
11. Double-click the Text Contains Rule component and in the Contains field, select Constant Value and type "Altiris" in the value field. Click OK.
12. In the Variable Name field, select the variable Incident.IncidentName. Click OK.
13. Click OK to close the Text Contains Rule editor.
14. Double-click the End component connected to the "Contains" output path.
15. Open its Mapping field, select Create Value, and set the value to "true" by checking the Value checkbox.
16. In the other End component, open its Mapping field, and select Create Value, but leave the Value checkbox unchecked.
17. This completes configuration of the model. Click OK to close.

Add to the Service Catalog

Incident Management is intended for break/fix-type of issues. The Service Catalog is intended for handling process, such as HR onboarding, password reset, equipment requests, things of that nature.

The Service Catalog is an important tool in ServiceDesk, in that it provides means to end-users to help themselves, therefore reducing the load on IT. The processes added perform consistently and can be reported against using the built-in reporting capability in ServiceDesk.

Adding to the Service Catalog requires the new process be built in Symantec Workflow, then added to the "menu" found in the ServiceCatalogCategoryInfo integration library.

Examples of process you can build are:

- An automated software request and approval process, where the end-user selects the software needed, then the process does automatic checking of licenses, automatic approval, and the final result is software is delivered and installed without IT personnel involvement
- A reset password process that automatically goes into Active Directory and updates that user's information

To add a process to the Service Catalog

1. Create the process in Symantec Workflow, and when tested and ready to publish, choose the option to Publish to Process Manager Forms, or Publish to Process Manager Services, depending on the type of project.
2. Select the catalog location and deploy. During deployment, set the permissions for the process from the Permissions tab. You can also set permissions for the service catalog process in the portal from the Admin tab > Service Catalog Settings. Select the Service Catalog item for which you want to set permissions, and select the Edit Form icon. Add users/groups from the Permissions tab accordingly.

Define New Reports

Several predefined reports that present useful information right out of the box. However, the administrator can modify these reports or create entirely new reports in from the Reports tab in ServiceDesk. See the ServiceDesk User's Guide for more information.

Reports are also used to filter the task list for a user.

Create a Standard Report

This example will create a standard report that lists all resolved incidents by the Respond Type. Additionally, it will show the primary contact, phone number, email, priority, and description of the incident.

To create a new report based off an existing report

1. Go to the Reports tab and select Incident Management from the Report Categories.
2. Select the plus icon and select Add Standard Report.
3. Add a name to your report: List Resolved Incidents by Respond Type.

4. The left pane of the report design screen is the Data List. The Data List represents data available to include in the report. As you select data items, the table will display on the right hand pane under Columns. Under the Data List select the following options:
    - Process Management - Add Processes to Report
    - Process Management - Include Process Actions
    - Process Management - Not Completed
    - Incident Management - Add Incident Management to Report
    - Incident Management - Add Custom Incident Data (leave additional filter criteria blank by clicking OK)
    - Incident Management - Add Custom Incident Data (leave additional filter criteria blank by selecting OK)
    - Process Contacts - Add Process Contacts to Report
    - Process Contacts - Primary Contact (leave additional filtering blank by selecting OK)
    - User - Add Users to Report
5. From the Columns List (right pane), select the following columns to display on your report:
    - User Table - First Name
    - User Table - Last Name
    - User Table - Primary Email
    - Process - Status
    - Incident - Description
    - Incident - ID
    - Incident - Priority
6. The middle pane is intended to show a preview of returned data, not all of the data that will be returned by the report.
7. Adjust your report by using the arrows on columns displayed in middle pane or by using the arrows next to the column labels in the column list on the right pane. You can also adjust the column width by using the sliding width function on the column.
8. Use the Options tab on the Data list to further customize your report. Select Group By = Respond Type (if available in your image otherwise select Priority) and Sort By= Priority.
9. Select the Description tab and create a description for your report: A list of all resolved incidents listed by respond type.
10. Select the Permissions tab and select the Add New Permissions button.
11. Search for and add Support I as a group that can view and edit this report.
12. Generate the report.
13. To make this report a chart rather than a graph, simply select the Chart option in the middle pane. From here you can select what type of chart you would like use along with other attributes. The view last selected for the report, chart or grid, will be the view for the report when run in ServiceDesk.

14. Save the report.
15. Check your report by making sure you have some resolved incidents. Login as a Support 1 user (technician1 or technician2) and check your report.

Creating a Child Report

Child reports are important for permissions and performance reasons. Child reports don't change the original report definition (the user designing the report can only add data). Since data cannot be removed, the report always contains the data the administrator intends on that user seeing. Child reports inherit the data and security of the parent report. It is recommended to create child reports for users. The "Add Child Report" is available from the Actions menu (orange lightning bolt) for the particular report.

Configure Automatic Generation of Reports

You can configure reports to be written to a file or e-mailed automatically by defining a reporting schedule.

To set up a reports schedule

1. In ServiceDesk, go to Admin > Reports > Report Schedule List.
2. Click on the Add button on the right.
3. Set up the schedule as desired and click Save.
4. From the schedule's actions (lightning bolt) icon, click Reports.
5. Click on Add Report and select the report(s) to include.
   - Select the user to run the reports as, if necessary
   - Select the destination type (file or email)
   - Enter the recipient e-mail address (separate multiple addresses using a semi-colon)
   - Select the output format
   - Name the report as desired
6. Click on Add.
7. Set up as many schedules as needed.
8. Next, it is necessary to enable the report for programmatic access (which creates a web service for the report). Complete the following instructions for the reports you wish to automatically generate.

Making a Report a Web Service

Every report in ServiceDesk has the ability to become a web service. The report is accessible like any other ServiceDesk process deployed as a web service. Follow these instructions if you wish to expose report data so it can be called via a web service.

To generate a web service for a report

1. From the Reports tab, select Edit Report Definition from the Actions menu for the particular report.
2. At the top of the Designer screen, click on Web Services.
3. Check the "Enable for Programmatic Access" checkbox, and populate the web service information fields.
4. Click on Generate.

Replicating ServiceDesk Data

The replication schedule tells ServiceDesk how often to either move or copy certain data to either a file or a database. You can set up as many schedules as needed to handle data. You can set up replication at any time (does not have to be upon initial implementation of ServiceDesk).

To set up data replication

1. In ServiceDesk, go to Admin > Reports > Replication Schedule List.
2. Click the Add New Replication Schedule icon.
3. Set up the schedule as desired.

Create a New Schedule

Schedules are used to record various ServiceDesk activities (primarily scheduled releases and scheduled changes). The core processes for Change Management and Release Management directly update the schedule/calendar visible under Knowledge Base > Schedules.

It is possible for an administrator to create a new schedule and allow users to add entries to track events entirely separate from the default schedule. You can also call the new schedule directly from a process.

To create a new schedule

1. In ServiceDesk, go to the Knowledge Base > Schedules page.
2. In the Schedule pane on the left, click on the Add Schedule icon (it will not appear unless the user has permission).
3. Enter a name for the new schedule, and if desired, select a color for scheduled items. For example, "Training Class Schedule."
4. Select Permissions > Add Permissions to set the criteria for schedule accessibility.
5. Click on Save. The new schedule appears in the Schedules pane.
6. Select the checkboxes for the schedules you wish to make visible in the calendar.

To call the schedule from a process and add an entry

1. You can add entries to any schedule from within a process using the AddScheduleEntry component. Open a ServiceDesk project in Symantec Workflow through which an entry to the schedule can be justifiably created. For example, a smart task that accesses a form to sign up users for training. The form UI feeds the

AddScheduleEntry component its data, then that component makes the connection to the calendar and creates the entry.

2. Add an AddScheduleEntry component to the appropriate model and make the necessary connections.
3. Double-click the AddScheduleEntry component.
4. On the Inputs tab, set the Service URL Source field to Use Default. This will utilize the source location to which the process is deployed.
5. For the Scheduled Source, select From Picker.
6. For Schedule, browse and select the appropriate schedule from the ScheduleEditorForm list. The entry will inherit the appearance and the permissions of the selected schedule.
7. Populate the Schedule Entry Title, Start Date, End Date, Description, Pop-Up Description, and Item Color fields.
8. Enter a name for the output variable on the Outputs tab. This completes the configuration.

Adding & Removing E-mail Notification

There are several e-mail notifications set up throughout Incident, Change, Problem, and Release Management, and the Knowledge Base process. You can add and remove these as needed. There are four methods for adding notifications:

- Use the Terminate and Transfer Dialog Flow component to call SD.EmailServices
- Use the Merge Text and HTTP Post components to call SD.EmailServices.
- Use the Send Email component within the process
- Create a custom Web Service Caller component to call SD.EmailServices (this requires an upgraded version of Symantec Workflow)

The recommended method for notifications is by calling SD.EmailServices. This way the behavior and appearance is consistent. The link to SD.EmailServices uses variables to provide the "Create Email URL," process ID, workflow tracking ID, and mailto. Recommended input parameters are: process ID, tracking ID, mailto, template, and an autosend value.

Here is an example of a URL calling SD.EmailServices, which can populate a "Terminate and Transfer" component:

[ProfileProperties].service_desk_settings_create_email_url?processid=[Global].ReportProcessID&trackingID=workflowTrackingId&Mailto=MailTo&InputTemplate=Autosend.Incident.StartChat&Autosend=True

The string above specifies the template name in SD.EmailServices, which is "Autosend.Incident.StartChat." If you open SD.EmailServices, and look at that model, you will see that it contains the e-mail content for inviting a participant to chat.

Disabling a notification is as simple as disabling the component that calls SD.EmailServices or disabling the Send Email component generating the unwanted notification. Every component has an "Is Enabled" setting that can be disabled to cause the component to become inactive. It is recommended to disable components rather than remove them, in case they are wanted in the future.

Application Property for Two Notifications

There are two settings in ServiceDesk that enable the notifications for incident creation (SendNotificationIncidentCreation) and incident resolution (SendNotificationIncidentResolution). You can disable these notifications by changing the application property for these to False.

Remove an Approval Step

In ServiceDesk, many approvals happen via the Dialog Workflow component which presents a user a form to either approve or deny something. For example, there is an approval step for deleting a Knowledge Base item. It is possible to bypass this approval step by disabling the component that handles the approval.

In general, Symantec recommends disabling unwanted components rather than deleting them. This example shows disabling the Dialog Workflow component; the method for disabling is the same for other components as well.

To disable the approval step for removing a Knowledge Base article

1. In Symantec Workflow, open the SD.KBSubmission project.
2. Click on the Removal Approval model in the Project tree on the left.
3. Double-click the "Review Removal Request" Dialog Workflow component.
4. Click on the Settings tab.
5. At the bottom, uncheck "Is Enabled" and select "Approved" as the Execution Outcome. Now any time a KB article is to be removed, the removal step will always return "true" as if approval was granted. There is no need for user interaction.

Customize the Spell Checking Dictionary

User input in ServiceDesk is validated for spelling typically by a SpellCheck component. The component is not visible to the end-user, however it creates red underlining for misspelled words. By right-clicking the misspelled word, a list of spelling suggestions appears. Selecting a suggestion corrects the misspelling.

There is also a SpellCheckButton component that appears as a button in the form (often displayed as a "Check Spelling" button). The component targets a specific component (for example, a Textbox). After entering information into the form and clicking this button, a standard spell check dialog window will display. The user can then ignore or change the words called out as misspelled.

Symantec Workflow uses "KaramaSoft's Ultimate Spell" technology for these two components. A custom dictionary can be added to Ultimate Spell, but only through altering the directory of the web application in ASP.NET. Therefore another option is to have users edit the spell checking dictionary utlized by their browser, such as the Google toolbar spell checking tool. The instructions below explain how to do this as an example.

The spell check tool in the Google toolbar appears as a green checkmark. Once you enter information into any web form, you can click the "Spell Check" button and form data entered will be assessed. To add misspelled words to the dictionary, right-click on the word and select "Add to Dictionary."

To configure the Google dictionary

1. Click Start > Run.
2. In the Run window, type "notepad %HOMEPATH%\Application Data\Google\User Dictionary.txt" (omitting the quotation marks), and click OK. (If this doesn't work, it is possible to browse to the directory, for example, C:\Documents and Settings\[user name]\Application Data\Google. "Application Data" is a hidden folder by default so it may be necessary to make it visible by going to Tools > Folder Options > View > Advanced Settings > Files and Folders > Hidden Files and Folders and select "show hidden files and folders.")
3. The dictionary opens as a text file in Notepad. The words addded to the dictionary display, and you can modify as needed.

Create Incidents from Other Sources

Notification Server

Incidents can be created from within Notification Server directly from an item by right-clicking the item and selecting the "Create Incident in ServiceDesk" option. Doing so launches a "Create New Incident" form tailored to Notification Server.

To enable this functionality, it is necessary to manually install the SD.Feeder.CreateIncidentForAssetInNS package and deploy it to the production server.

To install the SD.Feeder.CreateIncidentForAssetInNS package

1. In Symantec Workflow, click the Add button and browse to the list of ServiceDesk project packages.
2. Open the package for SD.Feeder.CreateIncidentForAssetInNS.
3. Deploy the project using the same deployment procedure as for other ServiceDesk projects to introduce this functionality.

Other Systems

The integration libary SD.Data shows all the attributes of the Incident Management data type. As long as a system can make the web service call to Incident Management and provide at a minimum the required data to make an incident, it is possible to create incidents via other access points to ServiceDesk.

Integrate ServiceDesk 7 with Other Systems

NOTE: This requires a full Symantec Workflow license.

Using the Integration Library, it is possible to generate custom components to integrate with databases and web services. This is a powerful option for extending the capability of ServiceDesk. For example, you could create a SoftwarePackagesLibrary SQL table component to read the inventory list of software to incorporate into a "Request Software" Service Catalog process.

There are many ways to take advantage of your existing data sources using the Integration Library capability. See the Symantec Workflow documentation for additional information.

Create a Web Part

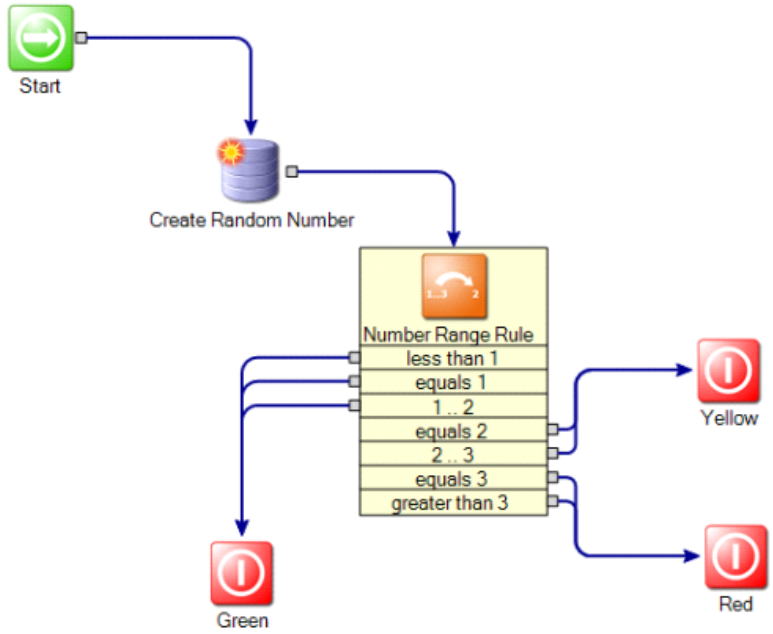
These example instructions create a new custom web part to add to a dashboard in ServiceDesk. The web part is created in a Web Forms project in Symantec Workflow. The web part is a simple stoplight that reads in a random number and based on the number, shows either red, yellow, or green.

To create a new web part (example)

1. Create a new Web Forms project. Name it indicative of what the web part will do, for example, "MyCompany.Dashboard.StopLight"
2. Add an "Add New Data Element" component and configure as follows:
   - Data Type - Number (Integer)
   - Output variable name - Counter
3. Add a Form Builder component, and connect the components accordingly:
4. Open the Form Builder component and configure as follows:

- When prompted, answer no to creating an outcome component.
- Add a Stoplight component to the form and resize it as desired. Configure it as follows:
  - Image states can remain as they are by default (red, yellow, green)
  - Set the default state to red
  - Open the Image Selection model for configuration
    - Clone the existing End component twice and rename them to Red, Yellow and Green and open each one to select the corresponding color option based on the name of the component
    - Add a "Create Random Number" component, and connect the Start component to it. Configure the "Create Random Number" component as follows:
    - Result name - ColorDecision
    - Check "Use min and max"
    - Min value = 1
    - Max value = 3
    - Add a "Number Range Rule" component and connect the Create Random Rule component to it. Configure the "Number Range Rule" component as follows:
    - Compare variable - ColorDecision (use the browse capability to pick this variable)
    - Handle Equals by - Make Explicit
    - Enter values 1, 2 and 3 in separate lines for comparison purposes.
    - Connect the "Number Range Rule" output paths in the following manner:
    - Less than 1, Equals 1 and 1..2 connected to Green end component.
    - Equals 2 and 2…3 connected to Yellow.
    - Equals 3 and Greater than 3 connected to Red.

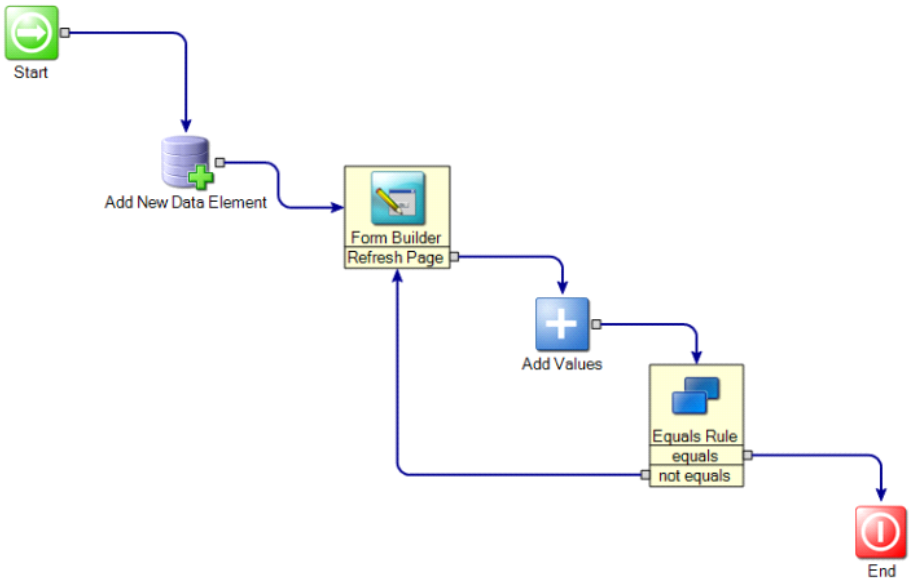
- Click OK to return to the Stoplight configuration dialog.
- Click OK to return to the Form Builder.



- Add an "Auto Exit Page on Timer" component to the form, and configure as follows:
- Refresh minutes = 0
- Refresh seconds = 5

- Click OK to return to the main model.

5. Add an "Add Values" component after the Form Builder, and connect the Form Builder component to the "Add Values" component. Configure as follows:
   - First value = Counter (use the browse capability to pick this variable)
   - Second value = 1 (constant)
   - Output value = Counter (use the browse capability to pick this variable)
6. Add an "Equals Rule" component after the "Add Values" component, and connect the "Add Values" component to the "Equals Rule." Configure the "Equals Rule" as follows:
   - Data Type = Number (integer)
   - Variable Name = Counter (use the browse capability to pick this variable)
   - Compare to = 10
7. Configure the output from the Equals Rule in the following manner:
   - Not equals connected to the Form Builder
   - Equals connected to the End Component



Settings for Publishing a Web Part

NOTE: This requires an upgraded version of Symantec Workflow.

When publishing, in order to make this project appear as a web part in the list of web parts available in ServiceDesk, use the following settings:

- Publish to Process Manager Forms
- Check "Is Web Part" checkbox

Note the category, as this is the category in which it will be found in ServiceDesk.

To insert the new web part into a page in ServiceDesk

1. Log in to ServiceDesk as the Administrator (or a user who has edit permission to a page).
2. From the Site Actions menu at the top of the portal, select Pages List.
3. Select the page in which you want to insert the web part from the Pages List on the left.
4. Click the Go To Page button.
5. From the Site Actions menu, select Modify Page.
6. From the Site Actions menu again, select Add Web Part.
7. Click on the category in which the web part was saved, then select its checkbox below the list of categories.
8. Select the zone, then click Add.
9. Click on Close.

10. If you put the page once again in Edit mode from the Actions menu, the web part will have an Actions (orange lightning bolt) menu, from which you can select Edit and further define the behavior of the web part.

Non-Changeable Items in Symantec Workflow Projects

While Symantec Workflow allows you to configure components and settings to correspond with the needs of your organization, some items should be left intact in order to maintain the integrity of the processes.

The following areas/items should not be modified at the project level:

- Main Project Settings - The name and Service ID of your project settings should never be modified or removed.
- Publishing –The Initialization and Workflow Type settings should be left as-is. These dictate how the process launches. Altering these could cause the process to fail.
- Reporting – The project reporting is configured specifically for data collection via Process Viewer. Altering the settings on this tab will compromise the reporting capabilities of your project.
- Libraries – Removing libraries from your project will in turn remove certain components and cause the process to fail.
- Global Data – Global data is data that is utilized throughout various stages of your process. Removing an item from the Global Data tab will compromise the output of the process and potentially cause failure to launch/run.
- Application Properties – This should be left enabled in order to maintain the link to ServiceDesk settings within the process.

The following areas/items should not be modified at the component level:

- Start – Removal of this component will cause the process to fail.
- End – Removal of this component will cause the process to fail.
- SetUp Process – This component establishes much of the criteria utilized by Process Viewer. Deleting or editing the component will compromise the reporting structure of your process.
- Global Logging Capture – This component turns on logging for your process. Removal of this component will mean that no exceptions or errors will be logged when your process is run.
- Create Log Message/Create Log Entry – These components allow for errors/issues to be properly logged and classified.
- Set Process State/Status – This component is placed after dialog workflows and is intended to be used to capture data for Process Viewer. The message associated with this component is displayed in Process Viewer to indicate what stage the process is in and has passed. While this component can be modified, particularly if the action being recorded needs to be clarified further, the actual status of “started”, “in progress”, or “completed” should not be altered.
- Add Process Reference – This component establishes criteria used in Process Viewer, such as what type of business service is affected by an incident. Deleting or editing the component will compromise the reporting structure of your process.

- Exception Component/Exception Trigger/Exception Trigger By Component/ Exception Trigger By Exception Type – These components are necessary for logging and reporting on any exception or issue that occurs while your process is being run. Removal of these will compromise your reporting capabilities as well as prevent you from troubleshooting properly.
- Add New Data Element – This component will most likely be configured so as to create a variable which will be utilized throughout the process. Removing this component will compromise the integrity of your project.

Scalability

ServiceDesk 7 is a complex system built on the most scalable elements of the Symantec software platform. There are several ways to configure ServiceDesk based on the needs of a particular organization. ServiceDesk supports simple configurations where one server provides all of the ServiceDesk capability and complex configurations that use clustering and load balancing technologies.

ServiceDesk 7 was designed and implemented as a modular system. There are two essential parts of ServiceDesk 7 that work together to present a cohesive Service Management platform to a user. Those pieces are the Process Manager Portal and the ServiceDesk 7 ITIL Processes. They each provide the following (the list below is not complete, but representative):

- ServiceDesk 7 Process Manager Portal:
  - Service Catalog
  - Knowledge Base
  - Calendars/Scheduling
  - Reporting
- ServiceDesk 7 ITIL Processes:
  - Incident Management
  - Problem Management
  - Change Management
  - Release Management

The Process Manager Portal is where almost all users will begin and end their work in ServiceDesk 7.

The information provided in this section will help you understand the different methods used to configure ServiceDesk servers to achieve optimal performance and user experience from the basic parts of the product.

ServiceDesk 7 always requires:

1.SQL Server Database

2.Notification Server 7 with CMDB Solution

These prerequisites should be installed on a separate server and each of the configurations described in this document assume this.

ServiceDesk 7 Configurations

ServiceDesk 7 is a memory-intensive, high volume transactional system. The minimum requirements for a ServiceDesk 7 are:

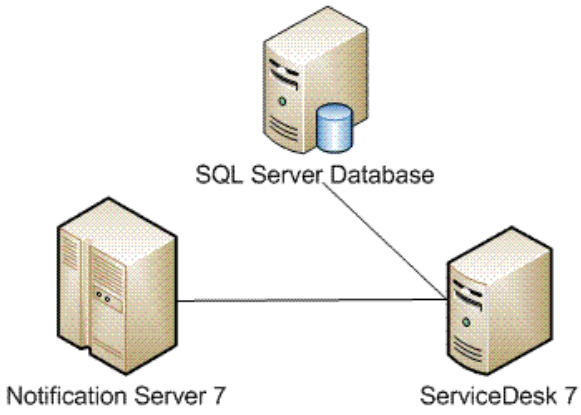
- Windows Server 2003 64 bit
- 16 GB RAM

It is always best to run SQL Server for ServiceDesk on a separate server.

There are additional software requirements that are outlined in the ServiceDesk Implementation Guide 7.0.

ServiceDesk 7 Simple

The most basic ServiceDesk 7 installation puts all of the services and processing for ServiceDesk 7 on a single application server. The Notification Server and the SQL Server Database should be on their own servers. This is a great starting point for any ServiceDesk installation, but exceeding the recommended number of concurrent users will quickly overwhelm the application server.



The number of concurrent users in the simple configuration is as follows:

- **Total users in the system (recommended maximum): 60,000**
- **Total groups in the system (recommended maximum): 30,000**
- **Concurrent end-users creating incidents: 100**
- **Concurrent technicians working in portal: 40**

These numbers are qualified by the following:

1. End-users create incidents affects the server (ITIL core), while technicians logging in and working affects the portal.
2. The concurrent use numbers represent load testing performed with a target of two second page response times.
3. Load testing was done against a single server wtih both the portal and ITIL processes installed, and database offbox.

ServiceDesk 7 Standard

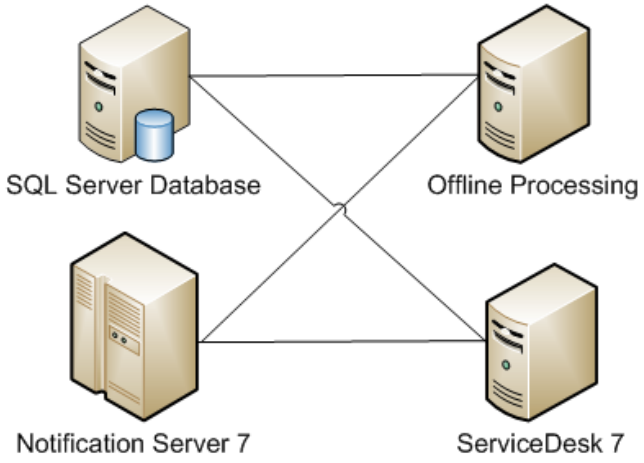
The first production configuration of ServiceDesk 7 involves moving all of the 'Offline/ Background Processing' onto a separate server. Background processing is work that doesn't have to be done in an immediate response to a user navigating the ServiceDesk. Examples of background processing are:

- E-mail Monitoring
- Task Timeouts
- Task Escalations
- Task Reminders
- Scheduled Reports
- Active Directory Synchronization

This configuration is ideal for customers who have fewer end-users who will access the Service Catalog in the portal directly, or rely heavily on e-mail interactions.

This configuration is the most straightforward of the advanced configurations because it is implemented by changing a small number of server settings and required only an additional server. This is very similar to 1. ServiceDesk 7 Simple, but the single end user facing application server has more capacity because it is only doing the work that is end user facing.

Note: The Offline processing server does not have to be a 64 bit server with 16 GB of RAM. It can be the customer's standard Application Server Specification.



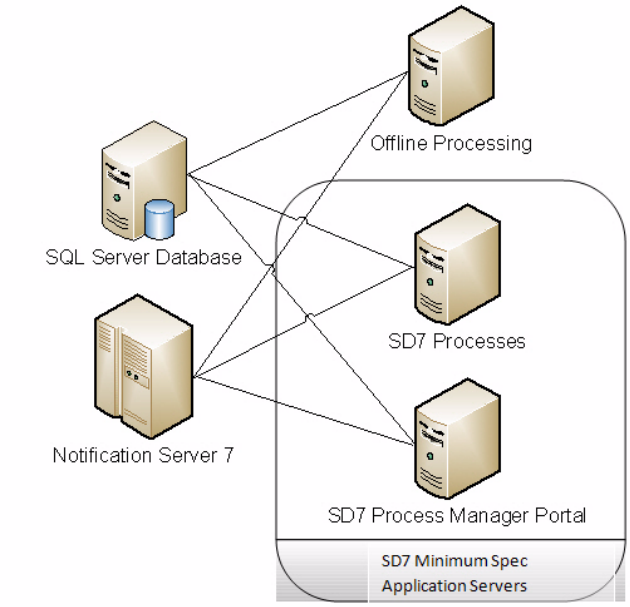
ServiceDesk 7 Advanced Configuration #1

The first advanced configuration of ServiceDesk 7 involves moving the SD7 Process Manager Portal onto a separate application server (this is the Worflow 7 Advanced Process Manager Portal modified for ServiceDesk 7). This configuration allows the system resources on the SD7 Process Manager portal to be utilized for caching database and web service calls access routinely. The SD7 Processes server runs all of the dynamic workflow processes that apply all of the business logic and rules of each of the ITIL 3 Service Desk processes.

Note: At this point in planning the physical topology of ServiceDesk 7 it is possible to introduce multiple SD7 Process Manager Portal Servers that are connected by an IP Load

Balancer. This does not allow for failover at this level. Failover in a load balanced environment requires the clustering capability.

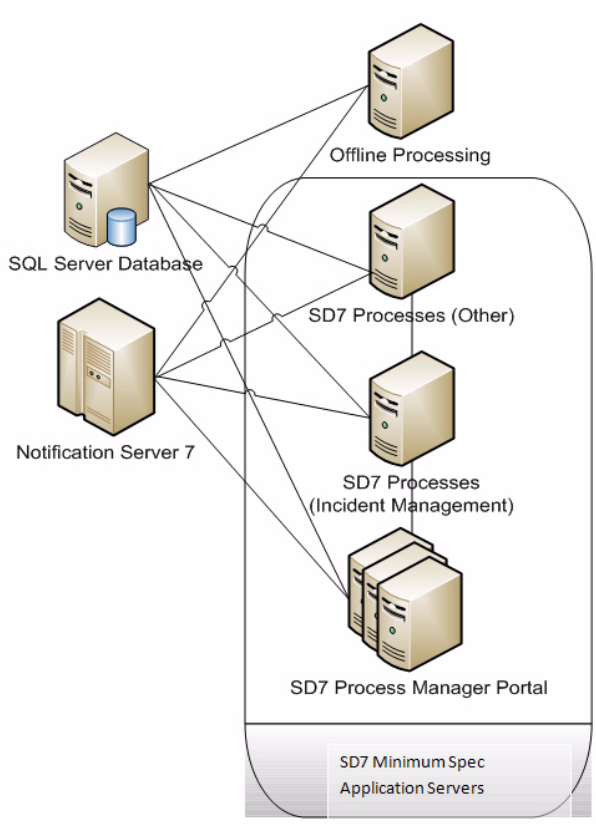
This configuration allows each server to handle more end users by focusing on a more specific module of the system that can beside the other pieces instead of within them. In this configuration the Process Manager portal has a dedicated server and the SD7 Process have a separate dedicated server. The two servers will communicate heavily as the SD7 Processes rely on the Process Manager Portal for things as critical as application settings, and the Process Manager portal will provide the end user pages that allow users to launch into the detail screens of the processes themselves.



ServiceDesk 7 Advanced Configuration #2

This configuration is very similar to Advanced Configuration 1 except that specific processes that are heavily leveraged can be moved to their own dedicated server. This will most commonly happen with SD7 Incident Management.

If you are putting heavily loaded (Many Users) processes onto dedicated servers, you will likely have multiple SD7 Process Manager Portals connected by an IP Load Balancer. This does not allow for failover at this level. Failover in a load balanced environment requires the clustering capability.



ServiceDesk 7 with Clustering for the Enterprise

Clustered configurations should be implemented with the help of a partner or professional services.